

Docket No.: H1658.0010/P010
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Keiichi Fukuda

Application No.: Not Yet Assigned

Filed: Concurrently Herewith

Art Unit: N/A

For: CONTENTS DATA
TRANSMISSION/RECEPTION SYSTEM,
CONTENTS DATA TRANSMITTER,
CONTENTS DATA RECEIVER AND
CONTENTS DATA
TRANSMISSION/RECEPTION METHOD

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following
prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Japan	2003-313852	September 5, 2003

Application No.: Not Yet Assigned

Docket No.: H1658.0010/P010

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 16, 2004

Respectfully submitted,

By 

Mark J. Thronson

Registration No.: 33,082

DICKSTEIN SHAPIRO MORIN &
OSHINSKY LLP

2101 L Street NW

Washington, DC 20037-1526

(202) 785-9700

Attorney for Applicant

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 9月 5日
Date of Application:

出願番号 特願2003-313852
Application Number:

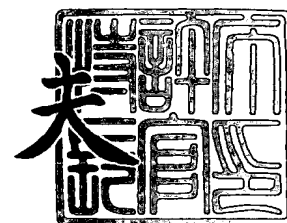
[ST. 10/C]: [JP 2003-313852]

出願人 株式会社デノン
Applicant(s):

2003年12月18日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2003-3105367

【書類名】 特許願
【整理番号】 DP3133
【提出日】 平成15年 9月 5日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 15/00
【発明者】
 【住所又は居所】 福島県白河市字老久保山 1 番地 1 株式会社デノン 白河ワーク
 ス内
 【氏名】 福田 圭一
【特許出願人】
 【識別番号】 301066006
 【氏名又は名称】 株式会社デノン
【代理人】
 【識別番号】 100074550
 【弁理士】
 【氏名又は名称】 林 實
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-279072
 【出願日】 平成14年 9月25日
【手数料の表示】
 【予納台帳番号】 155768
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータをキー情報を用いて暗号化し、前記キー情報を複数の信号路を介して前記コンテンツデータ受信装置に送信した後に暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信し、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信された前記キー情報を取得し、前記コンテンツデータ送信装置から複数の信号路を介して送信された前記暗号化したコンテンツデータを受信し、前記キー情報を用いて前記暗号化したコンテンツデータを復号することを特徴とするコンテンツデータ送受信システム。

【請求項 2】

コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するキー情報を生成するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報を用いて暗号化するコンテンツ暗号化部と、前記キー情報を複数の信号路を介してコンテンツデータ受信装置に送信すると共に前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記送信装置送受信部により前記キー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が抽出したキー情報を用いて暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータからキー情報を抽出し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ送受信システム。

【請求項 3】

コンテンツデータを送信するコンテンツデータ送信装置と当該コンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化に用いる複数のキー情報を生成すると共に複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報生成部が選択したキー情報を用いて暗号化するコンテンツ暗号化部と、前記複数のキー情報を複数の信号路及び前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータを送信する際に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、該送信装置送受信部により前記複数のキー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共にキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が選択したキー情報を用いて暗号化されたコ

ンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出して記憶部に記憶し前記受信装置送受信部が受信したキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からコンテンツデータの復号に用いるキー情報を選択し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ送受信システム。

【請求項 4】

請求項 2 及び請求項 3 記載のコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータ受信装置毎に割り当てられた受信装置 ID 情報を複数記憶する送信 ID 記憶部を有し、前記複数の受信装置 ID 情報のうちの 1 つの受信装置 ID 情報を選択すると共に前記コンテンツデータ受信装置から受信装置 ID 情報が一致した旨の情報が送信されてきたことを確認する送信装置 ID 認証部を備え、前記送信装置制御部は、前記送信装置 ID 認証部が選択した受信装置 ID 情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うと共に前記コンテンツデータ受信装置から受信装置 ID 情報が一致した旨の情報を受信したときに前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介してコンテンツデータ受信装置に送信する制御を行い、前記コンテンツデータ受信装置は、当該コンテンツデータ受信装置に割り当てられている受信装置 ID 情報を記憶する受信 ID 記憶部を有し、前記コンテンツデータ送信装置から送信された受信装置 ID 情報と前記受信 ID 記憶部が記憶する受信装置 ID 情報とを照合する受信装置 ID 認証部を備え、前記受信装置送受信部は、前記コンテンツデータ送信装置から送信された受信装置 ID 情報と前記受信 ID 記憶部に記憶した受信装置 ID 情報とが一致した場合に受信装置送受信部により信号路を介してコンテンツデータ送信装置に受信装置 ID 情報が一致した旨の情報を送信する制御を行うことを特徴とするコンテンツデータ送受信システム。

【請求項 5】

コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するためのキー情報を生成するキー情報生成部と、前記キー情報生成部が生成したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記キー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記キー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とするコンテンツデータ送信装置。

【請求項 6】

コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化のために用いる複数のキー情報を生成すると共に前記複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記キー情報生成部が選択したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記複数のキー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、前記複数のキー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号線を経由して前記コンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報を送信装置送受信部により前記コンテンツデータ

受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とするコンテンツデータ送信装置。

【請求項 7】

請求項 5 及び請求項 6 記載のコンテンツデータ送信装置において、コンテンツデータ受信装置毎に割り当てられた受信装置 ID 情報を複数記憶する送信 ID 記憶部を有し、複数の受信装置 ID 情報のいずれか 1 つの受信装置 ID 情報を選択すると共に前記コンテンツデータ受信装置から受信装置 ID 情報が一致した旨の情報が送信されてきたことを確認する送信装置 ID 認証部を備え、前記送信装置制御部は、前記受信装置 ID 情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うと共に前記コンテンツデータ受信装置から受信装置 ID 情報が一致した旨の情報を受信した後に前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うことを特徴とするコンテンツデータ送信装置。

【請求項 8】

コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が複数の信号路を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が抽出したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータからキー情報を抽出し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記キー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ受信装置。

【請求項 9】

コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が信号線を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共に複数のキー情報の中から暗号化に用いたキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が選択したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータから複数のキー情報を抽出し複数のキー情報の中からコンテンツデータの復号に用いるキー情報を選択し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記選択したキー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ受信装置。

【請求項 10】

請求項 8 及び請求項 9 記載のコンテンツデータ受信装置において、コンテンツデータ受信装置に割り当てられた受信装置 ID 情報を記憶する受信 ID 記憶部を有し、前記コンテンツデータ送信装置が送信した受信装置 ID 情報と前記受信 ID 記憶部が記憶している受信装置 ID 情報とを照合する受信装置 ID 認証部を備え、前記受信装置制御部は、コンテンツデータ送信装置が複数の信号路を介して送信した受信装置 ID 情報と前記受信 ID 記憶部に記憶された受信装置 ID 情報とが一致したときに受信装置 ID 情報が一致した旨の情報を受信装置送受信部により信号路を介して前記コンテンツデータ送信装置に送信する制御を行うことを特徴とするコンテンツデータ受信装置。

【請求項 11】

コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置 ID 情報をコンテンツデータ送信装置から複数の信号路を介してコンテ

ンツデータ受信装置に送信する第1ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ID情報をコンテンツデータ受信装置が有する受信装置ID情報と照合し受信装置ID情報が一致した場合に受信装置ID情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第2ステップと、コンテンツデータ受信装置から受信装置ID情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化したキー情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第3ステップと、コンテンツデータ送信装置から送信されたデータからキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第4ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき暗号化コンテンツデータをコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第5ステップとを有することを特徴とするコンテンツデータ送受信方法。

【請求項12】

コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置ID情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第1ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ID情報をコンテンツデータ受信装置が有する受信装置ID情報と照合し受信装置ID情報が一致した場合に受信装置ID情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第2ステップと、コンテンツデータ受信装置から受信装置ID情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化するための複数のキー情報を生成しコンテンツデータ送信装置からコンテンツデータ受信装置に送信する第3ステップと、コンテンツデータ送信装置から送信されたデータから複数のキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第4ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき前記複数のキー情報から暗号化に用いるキー情報を選択し当該選択したキー情報を用いてコンテンツデータを暗号化し暗号化したコンテンツデータと当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第5ステップと、コンテンツデータ送信装置から送信されてきたキー情報に関する情報に基づいて複数のキー情報の中からコンテンツデータの暗号化に用いたキー情報を選択しコンテンツデータ送信装置から送信されてきた暗号化されたコンテンツデータを復号する第6ステップとを有することを特徴とするコンテンツデータ送受信方法。

【書類名】 明細書

【発明の名称】 コンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置及びコンテンツデータ送受信方法

【技術分野】**【0001】**

本発明は、複数の装置間でオーディオデータやビデオデータ等のコンテンツデータを送受信するコンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置およびコンテンツデータ送信方法に関する。

【背景技術】**【0002】**

大容量のデータを記録することができる記録媒体としてデジタル・バーサタイル・ディスク (Digital Versatile Disc、以下「DVD」という。) がある。DVDには、ビデオデータとオーディオデータとを記録したDVD-VIDEOや、高音質のオーディオデータを記録したDVD-AUDIOがある。これらのDVDを再生する光ディスク再生装置は、DVDに記録されているデジタルデータを再生し、オーディオデータをアナログ信号としてアナログ出力したり、2チャンネルのデジタルデータとしてデジタル出力することができる。

【0003】

DVDには、レフト (L) チャンネル、ライト (R) チャンネル、サラウンドレフト (SL) チャンネル、サラウンドライト (SR) チャンネル、センター (C) チャンネルなどの複数のチャンネル (マルチチャンネル) のオーディオデータが記録されている場合がある。光ディスク再生装置は、DVDに記録されたマルチチャンネルのオーディオデータをデジタル出力する場合、マルチチャンネルのオーディオデータを2チャンネルのデジタルデータにダウンミックスし、ダウンミックスしたデータをIEC (International Electrotechnical Commission) 958のデータフォーマットに準拠したデジタルデータとして出力する。

【0004】

光ディスク再生装置からアナログ出力されるオーディオデータは、信号伝送中にノイズが重畳することにより音質が劣化することがある。光ディスク再生装置からデジタル出力されるオーディオデータは、アナログ出力のオーディオデータに比べ、信号伝送中のノイズの重畳による音質劣化がない。

【0005】

光ディスク再生装置からデジタル出力されるオーディオデータは、DVDに記録されているマルチチャンネルのオーディオデータを2チャンネルのオーディオデータに変換して出力しており、光ディスク再生装置から出力されたオーディオデータを増幅してスピーカ等へ出力する増幅装置 (例えば、オーディオビジュアル (Audio Visual、以下「AV」という。) アンプ) は、光ディスク再生装置からデジタル出力された2チャンネルのオーディオデータを受け取り、マルチチャンネルのオーディオデータに変換し出力する。

【0006】

増幅装置において、入力した2チャンネルのオーディオデータをマルチチャンネルのオーディオデータに変換する処理は、増幅装置に搭載された変換手段による演算により行われる。この演算処理は、その処理方法や演算に用いられるパラメータが変換手段 (例えば、デジタル・シグナル・プロセッサ (Digital Signal Processor、以下「DSP」という。)) の製造者毎に異なるため、入力した2チャンネルのオーディオデータをDVDに記録されている元のマルチチャンネルのオーディオデータに忠実に変換することができない。言い換えれば、2チャンネルのオーディオデータをマルチチャンネルのオーディオデータに変換することにより、光ディスクに記録されたマルチチャンネルのオーディオデータよりも音質が劣化したオーディオデータが増幅装置から出力されることになる。

【0007】

このため、マルチチャンネルのデジタルデータに上述の変換処理を行わずに、光ディス

ク再生装置により再生されたオーディオデータをマルチチャンネルのままデジタル出力し、デジタルデータの受け側である増幅装置が、マルチチャンネルのデジタルオーディオデータをアナログオーディオ信号に変換して出力することにより、光ディスクに記録された高音質のオーディオデータを忠実に再生したいという要望が高まっている。

【0008】

しかし、光ディスク再生装置からマルチチャンネルのデジタルオーディオデータを出力するようにした場合、このデジタルオーディオデータを記録媒体に複製記録することが可能になる。このデジタルオーディオデータの不正複製を防止するため、特許文献1に開示されているデータ伝送システムや、特許文献2に開示されているコンテンツ配布システムのような、2台の装置間で暗号化されたコンテンツデータを送受信する技術を用いることが考えられる。

【0009】

特許文献1に開示されているデータ伝送システムは、クライアントコンピュータが暗号キーと復号キーを生成し、サーバコンピュータに暗号キーと画像データ転送要求を送り、サーバコンピュータは、暗号キーにより画像データを暗号化し、暗号化した画像データをクライアントコンピュータに送信し、クライアントコンピュータは、保持している復号キーを用いて暗号化された画像データを復号化する。

【0010】

特許文献2に開示されているコンテンツ配布システムは、クライアントからサーバに、ユーザID、認証ID及びコンテンツデータのダウンロード要求が送信され、サーバのコンテンツサーバにユーザIDとコンテンツデータが登録されており、且つ、サーバが保持している認証IDとクライアントから送信された認証IDが同一である場合、サーバは、暗号化コンテンツを解読する解読鍵を生成し、暗号化コンテンツデータと解読鍵とをクライアントに送信する。クライアントは、サーバから送信された解読鍵を用いて暗号化コンテンツデータを解読し、コンテンツデータを再生する。

【0011】

【特許文献1】特開平11-289323号公報

【特許文献2】特開2000-242604号公報

【発明の開示】

【発明が解決しようとする課題】

【0012】

前述した特許文献1に開示されているデータ伝送システムや特許文献2に開示されているコンテンツ配布システムでは、コンテンツデータを1つのキー情報を用いて暗号化し、装置間を接続する単一の信号線を用いて、暗号化したコンテンツデータと暗号化したコンテンツデータの暗号を解読するための暗号解除情報（キー情報）を送信する。

【0013】

このようなシステムでは、コンテンツデータを1つのキー情報によってのみ暗号化し、この暗号解除情報（キー情報）を一塊りの情報として単一の信号線を介してコンテンツデータ送信装置からコンテンツデータ受信装置に送るため、2台の装置間で伝送されているデータの中からその情報を取り出し、その暗号解除情報を用いて暗号化コンテンツデータを復号し、元の高品質のコンテンツデータを得ることができるという問題がある。

【0014】

本発明は、装置間で送受信する暗号化されたコンテンツデータを復号するための暗号解除情報を抽出し容易に解読することができないコンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置及びコンテンツデータ送受信方法を提供することを目的とする。

【課題を解決するための手段】

【0015】

上記課題を解決するために、本願の請求項1の発明は、コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備

えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータをキー情報を用いて暗号化し、前記キー情報を複数の信号路を介して前記コンテンツデータ受信装置に送信した後に暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信し、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信された前記キー情報を取得し、前記コンテンツデータ送信装置から複数の信号路を介して送信された前記暗号化したコンテンツデータを受信し、前記キー情報を用いて前記暗号化したコンテンツデータを復号することを特徴とする。

【0016】

本願の請求項2の発明は、コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するキー情報を生成するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報を用いて暗号化するコンテンツ暗号化部と、前記キー情報を複数の信号路を介してコンテンツデータ受信装置に送信すると共に前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記送信装置送受信部により前記キー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が抽出したキー情報を用いて暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータからキー情報を抽出し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とする。

【0017】

本願の請求項3の発明は、コンテンツデータを送信するコンテンツデータ送信装置と当該コンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化に用いる複数のキー情報を生成すると共に複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報生成部が選択したキー情報を用いて暗号化するコンテンツ暗号化部と、前記複数のキー情報を複数の信号路及び前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータを送信する際に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、該送信装置送受信部により前記複数のキー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共にキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が選択したキー情報を用いて暗号化されたコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出して記憶部に記憶し前記受信装置送受信部が受

信したキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からコンテンツデータの復号に用いるキー情報を選択し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とする。

【0018】

本願の請求項4の発明は、請求項2及び請求項3記載のコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータ受信装置毎に割り当てられた受信装置ID情報を複数記憶する送信ID記憶部を有し、前記複数の受信装置ID情報のうちの1つの受信装置ID情報を選択すると共に前記コンテンツデータ受信装置から受信装置ID情報が一致した旨の情報が送信されてきたことを確認する送信装置ID認証部を備え、前記送信装置制御部は、前記送信装置ID認証部が選択した受信装置ID情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うと共に前記コンテンツデータ受信装置から受信装置ID情報が一致した旨の情報を受信したときに前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介してコンテンツデータ受信装置に送信する制御を行い、前記コンテンツデータ受信装置は、当該コンテンツデータ受信装置に割り当てられている受信装置ID情報を記憶する受信ID記憶部を有し、前記コンテンツデータ送信装置から送信された受信装置ID情報と前記受信ID記憶部が記憶する受信装置ID情報とを照合する受信装置ID認証部を備え、前記受信装置送受信部は、前記コンテンツデータ送信装置から送信された受信装置ID情報と前記受信ID記憶部に記憶した受信装置ID情報とが一致した場合に受信装置送受信部により信号路を介してコンテンツデータ送信装置に受信装置ID情報が一致した旨の情報を送信する制御を行うことを特徴とする。

【0019】

本願の請求項5の発明は、コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するためのキー情報を生成するキー情報生成部と、前記キー情報生成部が生成したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記キー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記キー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とする。

【0020】

本願の請求項6の発明は、コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化のために用いる複数のキー情報を生成すると共に前記複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記キー情報生成部が選択したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記複数のキー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、前記複数のキー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号線を経由して前記コンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報を送信装置送受信部により前記コンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とする。

【0021】

本願の請求項7の発明は、請求項5及び請求項6記載のコンテンツデータ送信装置において、コンテンツデータ受信装置毎に割り当てられた受信装置ID情報を複数記憶する送

信ID記憶部を有し、複数の受信装置ID情報のいずれか1つの受信装置ID情報を選択すると共に前記コンテンツデータ受信装置から受信装置ID情報が一致した旨の情報が送信されてきたことを確認する送信装置ID認証部を備え、前記送信装置制御部は、前記受信装置ID情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うと共に前記コンテンツデータ受信装置から受信装置ID情報が一致した旨の情報を受信した後に前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うことを特徴とする。

【0022】

本願の請求項8の発明は、コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が複数の信号路を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が抽出したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータからキー情報を抽出し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記キー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とする。

【0023】

本願の請求項9の発明は、コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が信号線を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共に複数のキー情報の中から暗号化に用いたキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が選択したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータから複数のキー情報を抽出し複数のキー情報の中からコンテンツデータの復号に用いるキー情報を選択し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記選択したキー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とする。

【0024】

本願の請求項10の発明は、請求項8及び請求項9記載のコンテンツデータ受信装置において、コンテンツデータ受信装置に割り当てられた受信装置ID情報を記憶する受信ID記憶部を有し、前記コンテンツデータ送信装置が送信した受信装置ID情報と前記受信ID記憶部が記憶している受信装置ID情報とを照合する受信装置ID認証部を備え、前記受信装置制御部は、コンテンツデータ送信装置が複数の信号路を介して送信した受信装置ID情報と前記受信ID記憶部に記憶された受信装置ID情報とが一致したときに受信装置ID情報が一致した旨の情報を受信装置送受信部により信号路を介して前記コンテンツデータ送信装置に送信する制御を行うことを特徴とする。

【0025】

本願の請求項11の発明は、コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置ID情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第1ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ID情報をコンテンツデータ受信装置が有する受信装置ID情報と照合し受信装置ID情報が一致した場合に受信装置ID情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第2ステップと、コンテンツデータ受信装置から受信装置I

D情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化したキー情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第3ステップと、コンテンツデータ送信装置から送信されたデータからキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第4ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき暗号化コンテンツデータをコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第5ステップとを有することを特徴とする。

【0026】

本願の請求項12の発明は、コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置ID情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第1ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ID情報をコンテンツデータ受信装置が有する受信装置ID情報と照合し受信装置ID情報が一致した場合に受信装置ID情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第2ステップと、コンテンツデータ受信装置から受信装置ID情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化するための複数のキー情報を生成しコンテンツデータ送信装置からコンテンツデータ受信装置に送信する第3ステップと、コンテンツデータ送信装置から送信されたデータから複数のキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第4ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき前記複数のキー情報から暗号化に用いるキー情報を選択し当該選択したキー情報を用いてコンテンツデータを暗号化し暗号化したコンテンツデータと当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第5ステップと、コンテンツデータ送信装置から送信されてきたキー情報に関する情報に基づいて複数のキー情報の中からコンテンツデータの暗号化に用いたキー情報を選択しコンテンツデータ送信装置から送信されてきた暗号化されたコンテンツデータを復号する第6ステップとを有することを特徴とする。

【発明の効果】

【0027】

本発明によれば、装置間で送受信する暗号化されたコンテンツデータを復号するための暗号解除情報を抽出し容易に解読することができないコンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置及びコンテンツデータ送受信方法を提供することができる。

【発明を実施するための最良の形態】

【0028】

図1は、本発明のコンテンツデータ送受信システムの一実施例を示す概略構成図である。

図1において、コンテンツデータ送受信システム10は、コンテンツデータ送信装置20とコンテンツデータ受信装置30とを備える。コンテンツデータ送受信システム10は、コンテンツデータ送信装置20がキー情報を用いてコンテンツデータを暗号化し、キー情報と暗号化したコンテンツデータ（暗号化コンテンツデータ）をコンテンツデータ受信装置30に送信し、コンテンツデータ受信装置30がコンテンツデータ送信装置20から送信されたキー情報と暗号化コンテンツデータとを受信し、キー情報を用いて暗号化コンテンツデータの暗号を解除するシステムである。

【0029】

コンテンツデータ送信装置20は、例えば、DVD等の記録媒体に記録されているビデオデータ及びオーディオデータを再生して出力するDVD-Videoプレーヤなどの再

生装置である。本実施例において、コンテンツデータ送信装置 20 は、再生装置として説明するが、ネットワークを介して伝送されるコンテンツデータを受信し、受信したコンテンツデータを出力する装置などであってもよい。

【0030】

コンテンツデータ受信装置 30 は、例えば、DVD-Video プレーヤから出力されたビデオデータ及びオーディオデータを受信し、ビデオデータをビデオ信号に変換してモニタ等の映像装置に出力し、オーディオデータをオーディオ信号に変換して増幅しスピーカに出力する AV (Audio Visual) アンプなどの増幅装置である。本実施例において、コンテンツデータ受信装置 30 は、増幅装置として説明するが、コンテンツデータ送信装置 20 から送信されたコンテンツデータを受信し、コンテンツデータを編集して出力する装置などであってもよい。

【0031】

コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 とは、ビデオデータを伝送するビデオデータ伝送路と、オーディオデータを伝送するオーディオデータ伝送路とにより接続されている。本実施例においては、ビデオデータ伝送路の説明を省略し、オーディオデータ伝送路についてのみ説明する。

【0032】

本実施例においては、図 1 に示すコンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 との間のオーディオデータ伝送路は、7 本の信号線で接続されているものとする。7 本の信号線うちの 6 本の信号線は、コンテンツデータ送信装置 20 からコンテンツデータ受信装置 30 にデータ（後述する接続確認データ、機器認証データ、キー情報送信データ及びコンテンツ送信データ）を送信する第 1 データ線～第 6 データ線であり、7 本の信号線のうち残りの 1 本の信号線は、コンテンツデータ受信装置 30 からコンテンツデータ送信装置 20 にデータ（後述する接続確認応答データ、機器認証応答データ、キー情報受信データ及びコンテンツ受信データ）を送信する応答線である。このようなオーディオデータ伝送路は、複数の信号線を伝送するデータとしてデジタル・オーディオ・インターフェースに準拠したフォーマットを利用することができる。なお、本実施例では、コンテンツデータ送信装置とコンテンツデータ受信装置との間のデータ伝送を信号線により行うものとして説明するが、それに限定されず、無線によりデータ伝送を行ってもよい。

【0033】

コンテンツデータ送信装置 20 は、コンテンツ再生部 21、コンテンツ暗号化部 22、キー情報生成部 23、送信装置 ID 認証部 24、送信装置送受信部 25、送信装置制御部 26 を備える。

【0034】

コンテンツ再生部 21 は、記録媒体に記録されたコンテンツデータ（オーディオデータ）を再生してコンテンツ暗号化部 22 に出力する。

【0035】

コンテンツ暗号化部 22 は、キー情報生成部 23 により生成されたキー情報を用いてコンテンツ再生部 21 が再生したコンテンツデータを暗号化する。コンテンツ暗号化部 22 における暗号化方法は、特に限定されずどのような方法でもよい。

【0036】

キー情報生成部 23 は、コンテンツデータを暗号化するキー情報を生成し、コンテンツ暗号化部 22 に出力する。キー情報は、例えば、複数ビットのデータ列からなる情報であり、キー情報の生成方法は特に限定されずどのような方法でもよい。

【0037】

また、キー情報生成部 23 は、生成したキー情報をコンテンツデータ受信装置 30 に送信する場合に、生成したキー情報を暗号化して送信装置送受信部 25 に出力する。

【0038】

キー情報生成部 23 におけるキー情報の暗号化は、予め定められた方法により行われる。後述するコンテンツデータ受信装置 30 のキー情報抽出部 33 は、コンテンツデータ送

信装置 20 のキー情報生成部 23 が行ったキー情報の暗号化を解除する復号処理機能を備え、キー情報生成部 23 が暗号化したキー情報は、後述するキー情報抽出部 33 により復号が可能である。本実施例では、キー情報生成部 23 がキー情報を暗号化してコンテンツデータ受信装置 30 に送信するが、暗号化せずにキー情報をコンテンツデータ受信装置 30 に送信するようにしてもよい。

【0039】

送信装置 ID 認証部 24 は、コンテンツデータ受信装置毎に固有に割り当てられた複数の受信装置 ID 情報を記憶する送信 ID 記憶部 24a を備える。送信装置 ID 認証部 24 は、後述する機器認証のときに、送信 ID 記憶部 24a に記憶された複数の受信装置 ID 情報の中から 1 つを選択し、受信 ID 情報を暗号化して送信装置送受信部 25 に出力する。

【0040】

送信装置 ID 認証部 24 における受信装置 ID 情報の暗号化方法は、特に限定されずどのような方法でもよい。後述するコンテンツデータ受信装置 30 の受信装置 ID 認証部 32 は、送信装置 ID 認証部 24 による受信装置 ID 情報の暗号化を解除する復号処理機能を備え、当該送信装置 ID 認証部 24 が暗号化した受信装置 ID 情報は、後述する受信装置 ID 認証部 32 により復号が可能である。本実施例では、送信装置 ID 認証部 24 が受信装置 ID 情報を暗号化してコンテンツデータ受信装置 30 に送信するが、暗号化せずに受信装置 ID 情報をコンテンツデータ受信装置 30 に送信するようにしてもよい。

【0041】

また、送信装置 ID 認証部 24 は、送信装置送受信部 25 が受信したコンテンツデータ受信装置 30 から送信されてきた受信装置 ID 情報と送信 ID 記憶部 24a に記憶している複数の受信装置 ID 情報とを照合し、照合した結果を送信装置制御部 26 に通知する。

【0042】

送信装置送受信部 25 は、送信装置制御部 26 の制御により、コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 との間の接続確認を行うためのデータ（接続確認データ及び接続確認応答データ）の送受信、機器認証を行うためのデータ（機器認証データ及び機器認証応答データ）の送受信、暗号化コンテンツデータの暗号を解除するキー情報に関するデータ（キー情報送信データ及びキー情報受信データ）の送受信、暗号化コンテンツデータの送受信に関するデータ（コンテンツ送信データ及びコンテンツ受信データ）の送受信を行う。

【0043】

後述するが、機器認証データ、キー情報送信データ及びコンテンツ送信データは、それぞれ複数のデータ列からなる。送信装置送受信部 25 は、送信装置制御部 26 の制御により、キー情報生成部 23 から出力される暗号化されたキー情報、送信装置 ID 認証部 24 から出力される暗号化された受信装置 ID 情報、コンテンツ暗号化部から出力される暗号化されたコンテンツデータをそれぞれ分割し、分割したそれぞれのデータを機器認証データ、キー情報送信データ、コンテンツ送信データが有する複数のデータ列にそれぞれ格納する処理を行い、それぞれのデータをコンテンツデータ受信装置 30 に送信する。

【0044】

送信装置制御部 26 は、コンテンツデータ送信装置 20 を総合的に制御する。送信装置制御部 26 は、操作部（図示せず）により再生開始の指示があると、コンテンツ再生部 21 における記録媒体に記録されているコンテンツデータの再生の制御を行う。

【0045】

送信装置制御部 26 は、コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 との間の接続確認及び機器認証が終了すると、キー情報生成部 23 においてコンテンツデータを暗号化するためのキー情報を生成する制御を行う。また、送信装置制御部 26 は、生成したキー情報を暗号化する制御を行う。

【0046】

送信装置制御部 26 は、コンテンツ暗号化部 22 において、コンテンツ再生部 21 が再

生したコンテンツデータをキー情報生成部 23 が生成したキー情報を用いて暗号化する制御を行う。

【0047】

送信装置制御部 26 は、送信装置送受信部 25 における接続確認データ及び接続確認応答データの送受信、機器認証データ及び機器認証応答データの送受信、キー情報送信データ及びキー情報受信データの送受信、コンテンツ送信データ及びコンテンツ受信データの送受信の制御を行う。

【0048】

送信装置制御部 26 は、コンテンツ暗号化部 22 が暗号化した暗号化コンテンツデータをコンテンツデータ受信装置 30 に送信する前に、コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 とが接続されていることを確認する接続確認データを、一本又は複数本のデータ線を介してコンテンツデータ受信装置 20 に送信する制御を行う。送信装置制御部 26 は、コンテンツデータ受信装置 30 から応答線を介して送信された接続確認応答データを受信すると、コンテンツデータ送信装置 30 とコンテンツデータ受信装置 20 との間が接続されていると判断する。

【0049】

送信装置制御部 26 は、コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 との間の接続確認が終了すると、送信装置 ID 認証部 24 の送信 ID 記憶部 24a に記憶されている複数の受信装置 ID 情報の中からコンテンツデータ受信装置 20 に対応する 1 つの受信装置 ID 情報を抽出し、当該受信装置 ID 情報を暗号化した受信装置 ID 情報を分割し、分割したそれぞれのデータを複数のデータ列からなる機器認証データにそれぞれ格納し、機器認証データを送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する制御を行う。

【0050】

送信装置制御部 26 は、送信装置 ID 認証部 24 がコンテンツデータ受信装置 30 から応答線を介して送信されてきた機器認証応答データに格納されている受信装置 ID 情報と、送信 ID 記憶部 24a に記憶してある受信装置 ID 情報とを照合した結果、両方の受信装置 ID 情報が一致している場合、機器認証を終了する。

【0051】

送信装置制御部 26 は、コンテンツデータ受信装置 30 から送信された受信装置 ID 情報と送信 ID 記憶部 24a に記憶してある受信装置 ID 情報とが一致していない場合、送信装置 ID 認証部 24 に、送信 ID 記憶部 24a に記憶されている複数の受信装置 ID 情報の中から、既に抽出した受信装置 ID 情報以外の受信装置 ID 情報を抽出させて暗号化させる制御を行う。そして、送信装置 ID 認証部 24 が暗号化した受信装置 ID 情報を分割し、分割したデータを複数のデータ列からなる機器認証データにそれぞれ格納し、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する制御を行う。

【0052】

送信装置制御部 26 は、機器認証が終了すると、キー情報生成部 23 が生成し暗号化したキー情報を分割し、分割したデータを複数のデータ列からなるキー情報送信データにそれぞれ格納し、キー情報送信データを送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する制御を行う。

【0053】

送信装置制御部 26 は、コンテンツデータ受信装置 30 から応答線を介して送信されてきたキー情報受信データに格納されている情報が、コンテンツデータ受信装置 30 においてキー情報を取得した旨の情報であるか否かの確認を行う。送信装置制御部 26 は、キー情報受信データに格納されている情報がキー情報を取得していない旨の情報の場合、再度キー情報送信データを送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する制御を行う。

【0054】

送信装置制御部 26 は、コンテンツデータ受信装置 30 がキー情報を取得したことを確認すると、コンテンツ暗号化部 22 により暗号化された暗号化データを分割し、分割したデータを複数のデータ列からなるコンテンツ送信データにそれぞれ格納し、コンテンツ送信データを送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する制御を行う。

【0055】

コンテンツデータ受信装置 30 は、受信装置送受信部 31、受信装置 ID 認証部 32、キー情報抽出部 33、コンテンツ復号化部 34、出力部 35、受信装置制御部 36 を備える。

【0056】

受信装置送受信部 36 は、コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 との間の接続確認のためのデータ（接続確認データ及び接続確認応答データ）の送受信、機器認証を行うためのデータ（機器認証データ及び機器認証応答データ）の送受信、暗号化コンテンツデータの暗号を解除するためのキー情報に関するデータ（キー情報送信データ及びキー情報受信データ）の送受信、暗号化コンテンツデータの送受信に関するデータ（コンテンツ送信データ及びコンテンツ受信データ）の送受信を行う。

【0057】

後述するが、機器認証応答データ、キー情報受信データ及びコンテンツ受信データは、それぞれ複数のデータ列からなる。受信装置送受信部 31 は、受信装置制御部 36 の制御により、キー情報抽出部 33 から送信装置送受信部 25 を介して出力されたキー情報を取得したか否かを示すデータ、送信装置 ID 認証部 32 から送信装置送受信部 25 を介して出力される受信装置 ID 情報が一致したか否かを示すデータ、コンテンツ暗号化部 22 から送信装置送受信部 25 を介して出力された暗号化コンテンツデータを取得したか否かを示すデータをそれぞれ分割し、分割したそれぞれのデータを機器認証応答データ、キー情報受信データ、コンテンツ受信データが有する複数のデータ列にそれぞれ格納する処理を行い、それぞれのデータをコンテンツデータ送信装置 20 に送信する。

【0058】

受信装置 ID 認証部 32 は、当該コンテンツデータ受信装置 30 に固有に割り当てられた受信装置 ID 情報を記憶する受信 ID 記憶部 32a を備える。受信装置 ID 認証部 32 は、機器認証のときに、コンテンツデータ送信装置 20 から送信されてきた受信装置 ID 情報と、受信 ID 記憶部 32a に記憶されている受信装置 ID 情報とを照合し、照合した結果を受信装置制御部 36 に通知する。

【0059】

受信装置 ID 認証部 32 は、コンテンツデータ送信装置 20 から送信されてきた受信装置 ID 情報と受信 ID 記憶部 32a に記憶されている受信装置 ID 情報とが一致している場合、受信装置制御部 36 の制御により、当該受信装置 ID 情報を暗号化して受信装置送受信部 31 に出力する。コンテンツデータ送信装置 20 から送信されてきた受信装置 ID 情報と受信 ID 記憶部 32a に記憶されている受信装置 ID 情報とが一致していない場合、受信装置 ID 認証部 32 は、受信装置 ID 情報が一致していない旨の情報（例えば、「0」のデータ）を暗号化して受信装置送受信部 31 に出力する。

【0060】

キー情報抽出部 33 は、受信装置送受信部 31 が受信したキー情報送信データに格納された情報から暗号化されたキー情報を抽出し、暗号化されたキー情報を復号してキー情報を取得する。キー情報抽出部 33 は、キー情報を取得できたか否かを受信装置制御部 36 に通知する。キー情報抽出部 33 は、受信装置制御部 36 の制御により、キー情報を取得できた場合、キー情報を抽出できた旨の情報として、例えば、「1」のデータを暗号化して受信装置送受信部 31 に出力し、キー情報を取得できなかった場合、キー情報を抽出できない旨の情報として、例えば、「0」のデータを暗号化して受信装置送受信部 31 に出力する。

【0061】

コンテンツ復号化部 34 は、受信装置送受信部 31 が受信したコンテンツ送信データから暗号化コンテンツデータを抽出し、キー情報抽出部 33 が抽出したキー情報を用いて暗号化コンテンツデータを復号（暗号を解除）する。

【0062】

出力部 35 は、コンテンツ復号化部 34 が復号したコンテンツデータをデジタルアナログ変換し、増幅してスピーカに出力する。

【0063】

受信装置制御部 36 は、コンテンツデータ受信装置 30 を総合的に制御する。受信装置制御部 36 は、受信装置送受信部 31 における接続確認データ及び接続確認応答データの送受信、機器認証データ及び機器認証応答データの送受信、キー情報送信データ及びキー情報受信データの送受信、コンテンツ送信データ及びコンテンツ受信データの送受信の制御を行う。

【0064】

受信装置制御部 36 は、受信装置送受信部 31 がコンテンツデータ送信装置 20 から送信された接続確認データを受信すると、接続確認応答データを受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する制御を行う。

【0065】

受信装置制御部 36 は、受信装置 ID 認証部 32 がコンテンツデータ送信装置 20 から送信されてきた機器認証データの受信装置 ID 情報と受信 ID 記憶部 32a に記憶されている受信装置 ID 情報とを照合した結果、両方の受信装置 ID 情報が一致している旨又は両方の受信装置 ID 情報が一致していない旨の情報をコンテンツデータ送信装置 20 に送信する制御を行う。

【0066】

両方の受信装置 ID 情報が一致している場合、受信装置制御部 36 は、受信装置 ID 認証部 32 に、受信装置 ID 情報を暗号化し、暗号化した受信装置 ID 情報を分割し、分割したデータを複数のデータ列からなる機器認証応答データにそれぞれ格納し、機器認証応答データを受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する制御を行う。

【0067】

両方の受信装置 ID 情報が一致しない場合、受信装置制御部 36 は、受信装置 ID 情報が一致しない旨の情報（例えば、「0」のデータ）を暗号化し、暗号化したデータを複数のデータ列からなる機器認証応答データにそれぞれ格納し、機器認証応答データを受信装置送受信部 25 から応答線を介してコンテンツデータ送信装置 20 に送信する制御を行う。

【0068】

受信装置制御部 36 は、キー情報抽出部 33 がコンテンツデータ送信装置 20 から送信されてきたキー情報送信データからキー情報を取得できたか否かを確認し、キー情報抽出部 33 がキー情報を取得できた旨又はキー情報抽出部 33 がキー情報を取得できなかった旨の情報をコンテンツデータ送信装置 20 に送信する制御を行う。

【0069】

キー情報抽出部 33 がキー情報を取得できた場合、受信装置制御部 36 は、キー情報を取得できた旨の情報（例えば、「1」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるキー情報受信データに格納し、キー情報受信データを受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する制御を行う。

【0070】

キー情報抽出部 33 がキー情報を取得できなかった場合、受信装置制御部 36 は、キー情報を取得できなかった旨の情報（例えば、「0」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるキー情報受信データに格納し、キー情報受信データを受信装置送受信部 31 から応答線を介してコンテンツデータ送信装

置 20 に送信する制御を行う。

【0071】

受信装置制御部 36 は、キー情報抽出部 33 がキー情報を取得でき、コンテンツデータ送信装置 20 からコンテンツ送信データが送信されてくると、コンテンツ送信データに格納されている暗号化コンテンツデータを抽出し、コンテンツ復号化部 34 においてキー情報を用いて暗号化コンテンツデータを復号する制御を行う。

【0072】

受信装置制御部 36 は、コンテンツ復号化部 34 がコンテンツデータ送信装置 20 から送信されてきたコンテンツ送信データから暗号化コンテンツデータを取得して復号できたか否かを確認し、コンテンツ復号化部 34 が暗号化コンテンツデータを受信し復号できた旨又はコンテンツ復号化部 34 が暗号化コンテンツデータを受信できなかった或いは復号できなかった旨の情報をコンテンツデータ送信装置 20 に送信する制御を行う。

【0073】

コンテンツ復号化部 34 が暗号化コンテンツデータを受信し復号できた場合、受信装置制御部 36 は、暗号化コンテンツデータを受信し復号できた旨の情報（例えば、「1」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるコンテンツ受信データに格納し、コンテンツ受信データを受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する制御を行う。

【0074】

コンテンツ復号化部 34 が暗号化コンテンツデータを受信できなかった或いは復号できなかった場合、受信装置制御部 36 は、暗号化コンテンツデータを受信できなかった或いは復号できなかった旨の情報（例えば、「0」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるコンテンツ受信データに格納し、コンテンツ受信データを受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する制御を行う。

【0075】

受信装置制御部 36 は、コンテンツ復号化部 34 において復号されたコンテンツデータをデジタルアナログ変換し、増幅して出力するよう出力部 35 を制御する。

【0076】

次に、コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 との間で伝送されるデータについて説明する。

図 2 は、本実施例のコンテンツデータ送受信システムにおける接続確認データ及び接続確認応答データのフォーマットを示す図である。図 2 (a) は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信する接続確認データを示し、図 2 (b) は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信する接続確認応答データを示す。

【0077】

接続確認データは、図 2 (a) に示すように、送信データ情報領域を備える。送信データ情報領域には、当該データが接続確認のためのデータ（接続確認データ）であることを示す情報が格納される。コンテンツデータ送信装置 20 は、図 2 (a) に示す接続確認データを複数のデータ線のうちの 1 線（本実施例では、第 1 データ線）を介してコンテンツデータ受信装置 30 に送信する。

【0078】

接続確認応答データは、図 2 (b) に示すように、送信データ情報領域を備える。送信データ情報領域には、当該データが接続確認データに対する応答データ（接続確認応答データ）であることを示す情報が格納される。コンテンツデータ受信装置 30 は、コンテンツデータ送信装置 20 からデータ線を介して図 2 (a) に示す接続確認データが送信されてくると、図 2 (b) に示す接続確認応答データを応答線を介してコンテンツデータ送信装置 20 に送信する。

【0079】

コンテンツデータ送信装置 20 は、接続確認データをコンテンツデータ受信装置 30 に送信した後、コンテンツデータ受信装置 30 から接続確認応答データが送信されてこない場合、コンテンツデータ受信装置 30 と接続されていないと判断し、一定時間後に再度送信を行う。

【0080】

図 3 は、本実施例のコンテンツデータ送受信システムにおける機器認証データ及び機器認証応答データのフォーマットを示す図である。図 3 (a) は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信する機器認証データを示し、図 3 (b) は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信する機器認証応答データを示す。

【0081】

機器認証データは、図 3 (a) に示すように、第 1 データ列、第 2 データ列、・・・、第 6 データ列からなる。各データ列は、暗号化された受信装置 ID 情報を分割した情報をそれぞれ格納するデータ領域と、機器認証データに関する情報を格納する送信データ情報領域とを備える。

【0082】

具体的には、第 1 データ列において、第 1 データ領域は、暗号化された受信装置 ID 情報を 6 分割した情報のうちのいずれか 1 つの情報 (第 1 ID 情報) を格納し、第 1 送信データ情報領域は、第 1 データ列～第 6 データ列のデータ列が機器認証データであることを示す情報を格納する。

【0083】

第 2 データ列～第 6 データ列において、第 2 データ領域～第 6 データ領域は、暗号化された受信装置 ID 情報を 6 分割した情報のうちのいずれかの情報 (第 2 ID 情報～第 6 ID 情報) をそれぞれ格納し、第 2 送信データ情報領域～第 6 送信データ情報領域は、機器認証データが第 1 データ列～第 6 データ列からなることを示す送信データ確認情報を格納する。

【0084】

送信データ確認情報は、例えば、チェックサム値である。チェックサム値は、データを 1 バイト (8 ビット) 毎に分け、各バイト単位で各ビット数を加算した結果を示す値である。本実施例では、第 2 データ列は、第 1 データ列と第 2 データ列のデータ領域に格納されているデータのチェックサム値と、第 1 データ列～第 6 データ列のデータ領域に格納されているデータのチェックサム値とを格納し、第 3 データ列～第 6 データ列は、それぞれのデータ列におけるデータ領域に格納されているデータのチェックサム値と、第 1 データ列～第 6 データ列のデータ領域に格納されているデータのチェックサム値とを格納するものとする。コンテンツデータ受信装置 30 は、送信データ確認情報のチェックサム値を確認することにより複数のデータ列からなる機器認証データを全て受信できたか否かを確認する。

【0085】

なお、本実施例では、第 1 データ列の第 1 送信データ情報領域は、第 1 データ列～第 6 データ列のデータ列が機器認証データであることを示す情報を格納し、第 2 データ列の第 2 送信データ情報領域～第 6 データ列の第 6 送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第 1 データ列の第 1 送信データ情報領域～第 5 データ列の第 5 送信データ情報領域に第 1 データ列～第 6 データ列のデータ列が機器認証データであることを示す情報を格納し、第 6 データ列の第 6 送信データ情報領域に第 1 データ列～第 6 データ列の送信データ確認情報 (第 1 データ列～第 6 データ列のチェックサム値) を格納してもよい。

【0086】

コンテンツデータ送信装置 20 は、送信 ID 記憶部 24 a が記憶している受信装置 ID 情報を暗号化し、暗号化した受信装置 ID 情報を分割し、図 3 (a) に示す第 1 データ列の第 1 データ領域～第 6 データ列の第 6 データ領域にそれぞれ第 1 ID 情報～第 6 ID 情

報を格納し、第1データ列～第6データ列をそれぞれ第1データ線～第6データ線を介して同時にコンテンツデータ受信装置30に送信する。

【0087】

機器認証応答データは、図3(b)に示すように、第1データ列、第2データ列、・・・、第6データ列からなる。各データ列は、コンテンツデータ受信装置30において受信装置ID情報が一致したか否かに関する情報を分割した情報のいずれかの情報を格納するデータ領域と、機器認証応答データに関する情報を格納する送信データ情報領域とを備える。

【0088】

具体的には、第1データ列の第1データ領域は、暗号化された受信装置ID情報を6分割した情報のうちのいずれか1つの情報(第1ID情報)を格納し、第1送信データ情報領域は、第1データ列～第6データ列のデータ列が機器認証応答データであることを示す情報を格納する。

【0089】

第2データ列の第2データ領域～第6データ列の第6データ領域は、暗号化された受信装置ID情報を6分割した情報のうちのいずれかの情報(第2ID情報～第6ID情報)をそれぞれ格納し、第2送信データ情報領域～第6送信データ情報領域は、機器認証データが第1データ列～第6データ列からなることを示す送信データ確認情報を格納する。送信データ確認情報は、機器確認データの第2データ列～第6データ列と同様に、例えば、チェックサム値である。

【0090】

なお、本実施例では、第1データ列の第1送信データ情報領域は、第1データ列～第6データ列のデータ列が機器認証応答データであることを示す情報を格納し、第2データ列の第2送信データ情報領域～第6データ列の第6送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第1データ列の第1送信データ情報領域～第5データ列の第5送信データ情報領域に第1データ列～第6データ列のデータ列が機器認証応答データであることを示す情報を格納し、第6データ列の第6送信データ情報領域に第1データ列～第6データ列の送信データ確認情報(第1データ列～第6データ列のチェックサム値)を格納してもよい。

【0091】

コンテンツデータ受信装置30において受信装置ID情報が一致したか否かを示す情報は、コンテンツデータ送信装置20が送信した受信装置ID情報とコンテンツデータ受信装置30に割り当てられている受信装置ID情報とが一致している場合は、コンテンツデータ受信装置30の受信ID記憶部32aに記憶されている受信装置ID情報を暗号化した情報である。当該情報は、分割され、分割された第1ID情報～第6ID情報は、第1データ列の第1データ領域～第6データ列の第6データ領域にそれぞれ格納される。

【0092】

また、コンテンツデータ送信装置20が送信した受信装置ID情報とコンテンツデータ受信装置30に割り当てられている受信装置ID情報とが一致していない場合は、コンテンツデータ受信装置30において受信装置ID情報が一致したか否かに関する情報は、全て「0」のデータであり、第1データ列の第1データ領域～第6データ列の第6データ領域に「0」のデータが格納される。

【0093】

本実施例では、コンテンツデータ送信装置20が送信した受信装置ID情報とコンテンツデータ受信装置30に割り当てられている受信装置ID情報とが一致している場合に、コンテンツデータ受信装置30において受信装置ID情報が一致したか否かに関する情報を、受信装置ID情報を暗号化した情報としたが、それ以外の情報(例えば、全て「1」のデータ)でもよい。また、本実施例では、コンテンツデータ送信装置20が送信した受信装置ID情報とコンテンツデータ受信装置30に割り当てられている受信装置ID情報とが一致していない場合に、コンテンツデータ受信装置30において受信装置ID情報

が一致したか否かに関する情報を全て「0」のデータとしたが、それ以外の情報（例えば、「101010・・・」のデータ）でもよい。

【0094】

コンテンツデータ受信装置30は、コンテンツデータ送信装置20から送信された機器認証データを受信すると、第1データ列～第6データ列に格納されている第1ID情報～第6ID情報を抽出し、これらの情報を復号し受信装置ID情報を取得し、受信装置ID認証部32の受信ID記憶部32aに記憶している受信装置ID情報と照合する。コンテンツデータ送信装置20から送信された受信装置ID情報と受信ID記憶部32aに記憶された受信装置ID情報が一致している場合、受信ID記憶部32aに記憶された受信装置ID情報を暗号化して分割し、図3(b)に示す第1データ列の第1データ領域～第6データ列の第6データ領域に格納し、応答線により、第1データ列～第6データ列を順次コンテンツデータ送信装置20に送信する。

【0095】

コンテンツデータ受信装置30からコンテンツデータ送信装置20への機器認証データの送信は、第1データ列を送信した後、予め定めた時間経過した後に第2データ列を送信するように、予め定めた時間毎に順次送信してもよい。

【0096】

機器認証データを応答線で第1データ列～第6データ列を連続して送信した場合、応答線から1つのデータ列として第1データ列～第6データ列とを抽出しやすくなり、抽出したデータから機器の受信装置ID情報を得ることができやすくなる。そうすると、受信装置ID情報により設定されている機器以外の機器（例えば、パーソナルコンピュータ）をDVDプレーヤに接続し、抽出した受信装置ID情報を用いて、パーソナルコンピュータをDVDプレーヤと認識させてキー情報や暗号化コンテンツデータを得て、暗号化コンテンツデータをキー情報により解読し、解読したコンテンツデータを違法に複製記録することができてしまう。

【0097】

このため、機器認証データの第1データ列を送信した後、予め定めた時間経過後に第2データ列を送信するように、第1データ列～第6データ列をそれぞれ予め定めた間隔毎に送信することにより、応答線から1つのデータ列としてID情報を抽出しにくくすることができる。

【0098】

図4は、本実施例のコンテンツデータ送受信システムにおけるキー情報送信データ及びキー情報受信データのフォーマットを示す図である。図4(a)は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信するキー情報送信データを示し、図4(b)は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信するキー情報受信データを示す。

【0099】

キー情報送信データは、図4(a)に示すように、第1データ列、第2データ列、・・・、第6データ列からなる。各データ列は、暗号化されたキー情報を分割した情報のいずれかの情報を格納するデータ領域と、キー情報送信データに関する情報を格納する送信データ情報領域とを備える。

【0100】

具体的には、第1データ列の第1データ領域は、暗号化されたキー情報を6分割した情報のうちのいずれかの1つの情報（第1キー情報）を格納し、第1送信データ情報領域は、第1データ列～第6データ列のデータ列がキー情報送信データであることを示す情報を格納する。

【0101】

第2データ列の第2データ領域～第6データ列の第6データ領域は、暗号化されたキー情報情報を6分割した情報のうちのいずれかの情報（第2キー情報～第6キー情報）をそれぞれ格納し、第2送信データ情報領域～第6送信データ情報領域は、キー情報送信デ

タが第1データ列～第6データ列からなることを示す送信データ確認情報を格納する。

【0102】

送信データ確認情報は、機器確認データの第2データ列～第6データ列と同様に、例えば、チェックサム値である。コンテンツデータ受信装置30は、送信データ確認情報のチェックサム値を確認することにより複数のデータ列からなるキー情報送信データを全て受信できたか否かを確認する。

【0103】

なお、本実施例では、第1データ列の第1送信データ情報領域は、第1データ列～第6データ列のデータ列がキー情報送信データであることを示す情報を格納し、第2データ列の第2送信データ情報領域～第6データ列の第6送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第1データ列の第1送信データ情報領域～第5データ列の第5送信データ情報領域に第1データ列～第6データ列のデータ列がキー情報送信データであることを示す情報を格納し、第6データ列の第6送信データ情報領域は、第1データ列～第6データ列の送信データ確認情報（第1データ列～第6データ列のチェックサム値）を格納してもよい。

【0104】

コンテンツデータ送信装置20は、図4（a）に示すように、暗号化したキー情報を6分割した情報をそれぞれ第1データ列の第1データ領域～第6データ列の第6データ領域に格納し、第1データ列～第6データ列をそれぞれ第1データ線～第6データ線で同時にコンテンツデータ受信装置103に送信する。

【0105】

キー情報受信データは、図4（b）に示すように、第1データ列、第2データ列、・・・、第6データ列からなる。各データ列は、キー情報を取得したか否かを示す情報を暗号化し、暗号化した情報を分割したいずれかの情報をそれぞれ格納するデータ領域と、キー情報受信データに関する情報を格納する送信データ情報領域とを備える。

【0106】

具体的には、第1データ列の第1データ領域は、キー情報を取得したか否かを示す情報を6分割した情報のうちのいずれか1つの情報（第1キー情報）を格納し、第1送信データ情報領域は、第1データ列～第6データ列のデータ列がキー情報受信データであることを示す情報を格納する。

【0107】

第2データ列の第2データ領域～第6データ列の第6データ領域は、キー情報を取得したか否かを示す情報を6分割した情報のうちのいずれかの情報（第2キー情報～第6キー情報）をそれぞれ格納し、第2送信データ情報領域～第6送信データ情報領域は、機器認証データが第1データ列～第6データ列からなることを示す送信データ確認情報を格納する。送信データ確認情報は、機器確認データの第2データ列～第6データ列と同様に、例えば、チェックサム値である。

【0108】

キー情報を取得したか否かを示す情報は、例えば、コンテンツデータ受信装置30がキー情報を取得した場合、全て「1」のデータであり、コンテンツデータ受信装置30がキー情報を取得できなかった場合、全て「0」のデータである。

【0109】

なお、本実施例では、第1データ列の第1送信データ情報領域は、第1データ列～第6データ列のデータ列がキー情報受信データであることを示す情報を格納し、第2データ列の第2送信データ情報領域～第6データ列の第6送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第1データ列の第1送信データ情報領域～第5データ列の第5送信データ情報領域に第1データ列～第6データ列のデータ列がキー情報受信データであることを示す情報を格納し、第6データ列の第6送信データ情報領域は、第1データ列～第6データ列の送信データ確認情報（第1データ列～第6データ列のチェックサム値）を格納してもよい。

【0110】

コンテンツデータ受信装置30は、コンテンツデータ送信装置20が送信したキー情報を取得できた場合、第1データ列の第1データ領域～第6データ列の第6データ領域の全てのビットに「1」のデータを格納し、コンテンツデータ送信装置20に応答線を介して、第1データ列～第6データ列を順次送信する。

【0111】

コンテンツデータ受信装置30は、コンテンツデータ送信装置20が送信したキー情報を取得できなかった場合、コンテンツデータ受信装置30は、第1データ列の第1データ領域～第6データ列の第6データ領域の全てのビットに「0」のデータを格納し、コンテンツデータ送信装置20に応答線を介して、第1データ列～第6データ列を順次送信する。

【0112】

本実施例では、キー情報の取得に関する情報は、コンテンツデータ受信装置30がキー情報の取得した場合に全て「1」のデータとし、コンテンツデータ受信装置30がキー情報の取得できなかった場合に全て「0」のデータとするが、それに限定されない。例えば、コンテンツデータ受信装置30がキー情報の取得した場合に、第1データ列の第1データ領域～第6データ列の第6データ領域の各データ領域の半分のビットを「1」のデータとし、残りの半分のビットを「0」のデータとするなど、キー情報を取得できた場合とキー情報を取得できなかった場合とが区別できれば、他のパターンのデータであってもよい。

【0113】

また、コンテンツデータ受信装置30がコンテンツデータ送信装置20に応答線を介してキー情報受信データを送信する際、上述した機器認証応答データの同様に、コンテンツデータ受信装置30は、第1データ列～第6データ列を、予め定めた時間間隔で順次送信してもよい。

【0114】

また、本実施例では、キー情報受信データは、複数のデータ列からなるものとしたが、キー情報を取得したか否かを示す情報を格納するデータ領域と、当該データ列がキー情報受信データであることを示す情報を格納する送信データ情報領域とからなる一つのデータ列であってもよい。

【0115】

図5は、本実施例のコンテンツデータ送受信システムにおけるコンテンツ送信データ及びコンテンツ受信データのフォーマットを示す図である。図5(a)は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信するコンテンツ送信データを示し、図5(b)は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信するコンテンツ受信データを示す。

【0116】

コンテンツ送信データは、図4(a)に示すように、第1データ列、第2データ列、・・・、第6データ列からなる。各データ列は、暗号化されたコンテンツデータを分割し、分割した情報のいずれかの情報を格納するデータ領域と、コンテンツ送信データに関する情報を格納する送信データ情報領域とを備える。

【0117】

具体的には、第1データ列の第1データ領域は、暗号化コンテンツデータを6分割した情報のうちのいずれかの1つの情報(第1コンテンツ情報)を格納し、第1送信データ情報領域は、第1データ列～第6データ列のデータ列がコンテンツ送信データであることを示す情報を格納する。

【0118】

第2データ列の第2データ領域～第6データ列の第6データ領域は、暗号化コンテンツデータを6分割した情報のうちのいずれかの情報(第2コンテンツ情報～第6コンテンツ情報)をそれぞれ格納し、第2送信データ情報領域～第6送信データ情報領域は、コンテ

ンツ送信データが第1データ列～第6データ列からなることを示す送信データ確認情報を格納する。

【0119】

送信データ確認情報は、キー情報送信データの第2データ列～第6データ列と同様に、例えば、チェックサム値である。コンテンツデータ受信装置30は、送信データ確認情報のチェックサム値を確認することにより複数のデータ列からなるコンテンツ送信データを全て受信できたか否かを確認する。

【0120】

なお、本実施例では、第1データ列の第1送信データ情報領域は、第1データ列～第6データ列のデータ列がコンテンツ送信データであることを示す情報を格納し、第2データ列の第2送信データ情報領域～第6データ列の第6送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第1データ列の第1送信データ情報領域～第5データ列の第5送信データ情報領域に第1データ列～第6データ列のデータ列がコンテンツ送信データであることを示す情報を格納し、第6データ列の第6送信データ情報領域は、第1データ列～第6データ列の送信データ確認情報（第1データ列～第6データ列のチェックサム値）を格納してもよい。

【0121】

本実施例では、暗号化されたコンテンツデータを分割し、分割したそれぞれの情報を各データ列の各データ領域に格納するとしたが、それに限定されない。例えば、コンテンツデータがマルチチャンネルのオーディオデータの場合、レフト、ライト、サラウンドレフト、サラウンドライト、センター、サブウーハーのオーディオデータは、それぞれチャンネル毎に暗号化され、暗号化レフト、暗号化ライト、暗号化サラウンドレフト、暗号化サラウンドライト、暗号化センター、暗号化サブウーハーのデータとなり、これらの暗号化コンテンツデータをそれぞれ第1データ列の第1データ領域～第6データ列の第6データ領域にそれぞれ格納するようにしてもよい。

【0122】

コンテンツデータ送信装置20は、図5（a）に示すように、第1データ列の第1データ領域～第6データ列の第6データ領域に、暗号化コンテンツデータをそれぞれ格納し、第1データ列～第6データ列をそれぞれ第1データ線～第6データ線を介して同時にコンテンツデータ受信装置30に送信する。

【0123】

本実施例においては、コンテンツデータ送信装置20からコンテンツデータ受信装置30への暗号化コンテンツデータの送信は、上述したように、暗号化コンテンツデータをデータ領域と送信データ情報領域とからなるデータ列に格納し、第1データ列～第6データ列を1回の送信として行うが、1回目には送信データ情報領域のみからなるデータ列をヘッダとして送信し、そのデータ列に連続してデータ領域のみからなるデータ列を送信する方法であってもよい。

【0124】

この場合、2回目以降のコンテンツ送信データの送信において、1回の送信により送信できる暗号化コンテンツデータのデータ量が、上述した図5（a）のフォーマットで送信する暗号化コンテンツデータのデータ量より多いため、コンテンツデータ送信装置20からコンテンツデータ受信装置30に、より短時間ので多くの暗号化コンテンツデータを送信することができる。

【0125】

コンテンツ受信データは、図5（b）に示すように、第1データ列、第2データ列、・・・、第6データ列からなる。各データ列は、暗号化コンテンツデータを受信できた否かを示す情報を暗号化し、暗号化した情報を分割したいずれかの情報をそれぞれ格納するデータ領域と、コンテンツ受信データに関する情報を格納する送信データ情報領域とを備える。

【0126】

具体的には、第1データ列の第1データ領域は、暗号化コンテンツデータを受信できたか否かを示す情報を6分割した情報のうちのいずれか1つの情報（第1コンテンツ情報）を格納し、第1送信データ情報領域は、第1データ列～第6データ列のデータ列がコンテンツ受信データであることを示す情報を格納する。

【0127】

第2データ列の第2データ領域～第6データ列の第6データ領域は、暗号化コンテンツデータを受信できたか否かを示す情報を6分割した情報のうちのいずれかの情報（第2コンテンツ情報～第6コンテンツ情報）をそれぞれ格納し、第2送信データ情報領域～第6送信データ情報領域は、コンテンツ受信データが第1データ列～第6データ列からなることを示す送信データ確認情報を格納する。送信データ確認情報は、キー情報受信データの第2データ列～第6データ列と同様に、例えば、チェックサム値である。

【0128】

なお、本実施例では、第1データ列の第1送信データ情報領域は、第1データ列～第6データ列のデータ列がコンテンツ受信データであることを示す情報を格納し、第2データ列の第2送信データ情報領域～第6データ列の第6送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第1データ列の第1送信データ情報領域～第5データ列の第5送信データ情報領域に第1データ列～第6データ列のデータ列がコンテンツ受信データであることを示す情報を格納し、第6データ列の第6送信データ情報領域は、第1データ列～第6データ列の送信データ確認情報（第1データ列～第6データ列のチェックサム値）を格納してもよい。

【0129】

暗号化コンテンツデータを受信できたか否かを示す情報は、例えば、コンテンツデータ受信装置30が暗号化コンテンツデータを受信した場合、全て「1」のデータであり、コンテンツデータ受信装置30が暗号化コンテンツデータを受信できなかった場合、全て「0」のデータである。

【0130】

コンテンツデータ受信装置30は、コンテンツデータ送信装置20が送信した暗号化コンテンツデータを受信できた場合、第1データ列の第1データ領域～第6データ列の第6データ領域の全てのビットに「1」のデータを格納し、コンテンツデータ送信装置20に応答線を介して、第1データ列～第6データ列を順次送信する。

【0131】

コンテンツデータ受信装置30は、コンテンツデータ送信装置20が送信した暗号化コンテンツデータを受信できなかった場合、コンテンツデータ受信装置30は、第1データ列の第1データ領域～第6データ列の第6データ領域の全てのビットに「0」のデータを格納し、コンテンツデータ送信装置20に応答線を介して第1データ列～第6データ列を順次送信する。

【0132】

本実施例では、キー情報の取得に関する情報は、コンテンツデータ受信装置30が暗号化コンテンツデータを受信した場合に全て「1」のデータとし、コンテンツデータ受信装置20が暗号化コンテンツデータを受信できなかった場合に全て「0」のデータとするが、それに限定されない。例えば、コンテンツデータ受信装置20が暗号化コンテンツデータを受信した場合に、第1データ列の第1データ領域～第6データ列の第6データ領域の各データ領域の半分のビットを「1」のデータとし、残りの半分のビットを「0」のデータとするなど、暗号化コンテンツデータを受信できた場合と暗号化コンテンツデータを受信できなかった場合とが区別できれば、他のパターンのデータであってもよい。

【0133】

また、コンテンツデータ受信装置30がコンテンツデータ送信装置20に応答線を介してコンテンツ受信データを送信する際、上述した機器認証応答データの同様に、コンテンツデータ受信装置30は、第1データ列～第6データ列を、予め定めた時間間隔で順次送信してもよい。

【0134】

また、本実施例では、コンテンツ受信データは、複数のデータ列からなるものとしたが、暗号化コンテンツデータを受信したか否かを示す情報を格納するデータ領域と、当該データ列がコンテンツ受信データであることを示す情報を格納する送信データ情報領域とからなる一つのデータ列であってもよい。

【0135】

また、本実施例では、コンテンツ受信データは、コンテンツデータ受信装置30がコンテンツ送信データを受信する毎にコンテンツデータ送信装置20に送信するものとしたが、それに限定されない。コンテンツデータ送信装置20がコンテンツ送信データの送信を開始した後、コンテンツデータ受信装置30は、予め定めた時間毎にコンテンツデータ送信装置20にコンテンツ受信データを送信するようにしてもよい。または、コンテンツデータ送信装置20がコンテンツ送信データの送信を開始した後、コンテンツデータ受信装置30は、コンテンツ送信データを受信する間隔が予め定めた時間以上経過した場合にコンテンツデータ送信装置20にコンテンツ受信データを送信するようにしてもよい。

【0136】

次に、本実施例のコンテンツデータ送受信システムにおけるデータの送受信の流れについて説明する。

図6は、本発明のコンテンツデータ送受信方法の一実施例を説明するための図である。図6において、図の縦軸は、時間の流れを示す。

【0137】

コンテンツデータ送信装置20は、コンテンツデータ送信装置20とコンテンツデータ受信装置30とが信号線により接続されているか否かを確認するため、図2(a)に示す接続確認データを、送信装置送受信部25から第1データ線～第6データ線を介してコンテンツデータ受信装置30に送信する。

【0138】

コンテンツデータ受信装置30は、受信装置送受信部31がコンテンツデータ送信装置20から送信された接続確認データを受信すると、図2(b)に示す接続確認応答データを受信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0139】

コンテンツデータ送信装置20は、送信装置送受信部25がコンテンツデータ受信装置30から送信された接続確認応答データを受信すると、送信装置ID認証部24の送信ID記憶部24aに記憶しているコンテンツデータ受信装置毎に固有に割り当てられている複数の受信装置ID情報から1つの受信装置ID情報を抽出し、抽出した受信装置ID情報を暗号化し、暗号化した受信装置ID情報を分割して図3(a)に示す機器認証データに格納し、送信装置送受信部25から第1データ線～第6データ線を介してコンテンツデータ受信装置30に送信する。

【0140】

コンテンツデータ受信装置30は、受信装置送受信部31がコンテンツデータ送信装置20から送信された機器認証データを受信すると、機器認証データの中からID情報領域に格納されている受信装置ID情報を抽出し、抽出した受信装置ID情報を復号し、復号した受信装置ID情報と受信装置ID認証部32の受信ID記憶部32aに記憶されている受信装置ID情報とを照合する。

【0141】

機器認証データから抽出した受信装置ID情報と受信ID記憶部32aに記憶している受信装置ID情報とが一致した場合、コンテンツデータ受信装置30は、当該受信装置ID情報を暗号化し、暗号化したデータを分割し、図3(b)に示す機器認証応答データに格納し、受信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0142】

機器認証データから抽出した受信装置ID情報と受信ID記憶部32aに記憶している

受信装置 ID 情報とが一致しない場合、コンテンツデータ受信装置 30 は、受信 ID 情報が一致しない旨の情報（例えば、全て「0」のデータ）を暗号化し、暗号化したデータを分割して図 3（b）に示す機器認証応答データに格納し、受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する。

【0143】

コンテンツデータ送信装置 20 は、送信装置送受信部 25 がコンテンツデータ受信装置 30 から送信された機器認証応答データを受信すると、機器認証応答データに格納されているデータを抽出し、そのデータからコンテンツデータ受信装置 30 において受信情報 ID 情報が一致したか否か確認する。

【0144】

機器認証データから得たデータがコンテンツデータ受信装置 30 において受信装置 ID 情報が一致した旨の情報の場合、コンテンツデータ送信装置 20 は、コンテンツ再生部 21 においてコンテンツデータの再生を開始し、コンテンツ暗号化部 22 においてキー情報生成部 23 がキー情報を用いてコンテンツデータを暗号化する処理を開始する。

【0145】

コンテンツデータ送信装置 20 は、コンテンツデータの暗号化を開始すると共に、キー情報生成部 23 により生成されたキー情報を暗号化し、暗号化したデータを分割して図 4（a）に示すキー情報送信データに格納し、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0146】

機器認証データから得たデータがコンテンツデータ受信装置 30 において受信装置 ID 情報が一致しない旨の情報の場合、コンテンツデータ送信装置 20 は、送信装置 ID 認証部 24 の送信 ID 記憶部 24 a に記憶している複数の受信装置 ID 情報の中から、既にコンテンツデータ受信装置 30 に送信した受信装置 ID 情報を除く受信装置 ID 情報の中から 1 つの受信装置 ID 情報を抽出し、その受信装置 ID 情報を暗号化し、暗号化したデータを分割して図 3（a）に示す機器認証データに格納し、再度、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。コンテンツデータ送信装置 20 は、コンテンツデータ受信装置 30 に割り当てられた受信装置 ID 情報と一致するまでこの処理を繰り返し行う。

【0147】

コンテンツデータ受信装置 30 は、受信装置送受信部 31 がコンテンツデータ送信装置 20 から送信されたキー情報送信データを受信すると、キー情報送信データの中からキー情報領域に格納されているデータを抽出し、抽出したデータを復号化しキー情報を取得する。このキー情報が暗号化コンテンツデータの暗号を解除する暗号解除情報となる。

【0148】

キー情報送信データからキー情報を取得することができた場合、コンテンツデータ受信装置 30 は、キー情報を取得した旨の情報（例えば、全て「1」のデータ）を暗号化し、暗号化したデータを分割して図 4（b）に示すキー情報受信データに格納し、受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する。

【0149】

キー情報送信データからキー情報を取得できなかった場合、コンテンツデータ受信装置 30 は、キー情報を取得できなかった旨の情報（例えば、全て「0」のデータ）を暗号化し、暗号化したデータを分割して図 4（b）に示すキー情報受信データに格納し、受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する。

【0150】

コンテンツデータ送信装置 20 は、送信装置送受信部 25 がコンテンツデータ受信装置 30 から送信されたキー情報受信データを受信すると、キー情報受信データの受信データ領域に格納されているデータを抽出し、コンテンツデータ受信装置 30 がキー情報を取得したか否かを確認する。

【0151】

コンテンツデータ受信装置 30 においてキー情報を取得できなかった場合、コンテンツデータ送信装置 20 は、再度、キー情報送信データを送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0152】

コンテンツデータ受信装置 30 においてキー情報を取得できた場合、コンテンツデータ送信装置 20 は、コンテンツ暗号化部 22 により暗号化した暗号化コンテンツデータを分割し、分割したデータを図 5 (a) に示すコンテンツ送信データに格納し、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0153】

コンテンツデータ受信装置 30 においてキー情報を取得できなかった場合、コンテンツデータ受信装置 30 は、コンテンツデータを取得できなかった旨の情報（例えば、全て「0」のデータ）を暗号化し、暗号化したデータを分割して図 5 (b) に示すコンテンツ受信データに格納し、受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する。

【0154】

コンテンツデータ受信装置 30 は、受信装置送受信部 31 がコンテンツデータ送信装置 20 から送信されたコンテンツ送信データを受信すると、コンテンツ送信データに格納されている暗号化コンテンツデータを抽出し、コンテンツ復号化部 34 においてキー情報抽出部 33 が抽出したキー情報を用いて暗号化コンテンツデータを復号化し、出力部 35 に出力する。

【0155】

出力部 35 は、コンテンツ復号化部 34 から出力されたコンテンツデータに対して、デジタルアナログ変換や増幅等を行い出力する。

【0156】

コンテンツデータ受信装置 30 は、コンテンツデータ送信装置 20 が送信したコンテンツ送信データを受信し暗号化コンテンツデータを復号すると、暗号コンテンツデータを取得した旨の情報を暗号化し、暗号化したデータを分割して図 5 (b) に示すコンテンツ受信データに格納し、受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する。

【0157】

コンテンツデータ送信装置 20 は、コンテンツデータ受信装置 30 から送信されたコンテンツ受信データを受信すると、コンテンツ受信データに格納されているコンテンツデータを取得した旨の情報からコンテンツデータ受信装置 30 がコンテンツデータを取得できたか否かを確認する。

【0158】

コンテンツデータ送信装置 20 は、コンテンツデータ受信装置 30 がコンテンツデータを取得できた場合、次の暗号化コンテンツデータを図 5 (a) に示すコンテンツ送信データに格納し、コンテンツ送信データを送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0159】

コンテンツデータ送信装置 20 は、コンテンツデータ受信装置 30 がコンテンツデータを取得できなかった場合、送信したコンテンツ送信データを、再度、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0160】

このようにして、コンテンツデータ送信装置 20 からコンテンツデータ受信装置 30 にコンテンツデータを送信する。

【0161】

以上のように、コンテンツデータ送受信システムにおいて、コンテンツデータ送信装置は、機器認証を行うための受信装置 ID 情報、コンテンツデータを復号するためのキー情

報、コンテンツデータを暗号化し、暗号化したデータを複数のデータ列からなるそれぞれのデータに格納し、そのデータを複数の信号線を用いてコンテンツデータ受信装置に送信する。

【0162】

このことにより、コンテンツデータ送信装置が出力する受信装置ID情報、キー情報、暗号化コンテンツデータを単一の信号線から取得することができないため、不正に受信装置ID情報、キー情報、暗号化コンテンツデータを得て、暗号化コンテンツデータをキー情報を用いて復号してコンテンツデータの違法複製することを防止することができる。

【0163】

前述した実施例では、コンテンツデータ送信装置20は、コンテンツデータを1つのキー情報を用いて暗号化し、コンテンツデータ受信装置30は、コンテンツデータ送信装置20から送信されてきた1つのキー情報を用いて暗号化コンテンツデータを復号化しているが、コンテンツデータの暗号化を複数のキー情報を用いて行うようにしてもよい。

【0164】

本発明において、コンテンツデータの暗号化を複数のキー情報を用いて行う場合の実施例について説明する。

図7は、本発明のコンテンツデータ送受信システムの他の実施例を示す概略構成図である。

コンテンツデータ送信装置20は、コンテンツ再生部21、コンテンツ暗号化部22、キー情報生成部23、送信装置ID認証部24、送信装置送受信部25、送信装置制御部26を備える。このうち、コンテンツ再生部21、コンテンツ暗号化部22、送信装置ID認証部24及び送信装置制御部26は、前述した実施例のコンテンツデータ送信装置20のコンテンツ再生部21、コンテンツ暗号化部22、送信装置ID認証部24及び送信装置制御部26と同様の構成であるため、説明を省略する。

【0165】

キー情報生成部23は、コンテンツデータの暗号化に用いる複数のキー情報を生成する。キー情報は、例えば、複数ビットのデータ列からなる情報であり、キー情報の生成方法は特に限定されずどのような方法でもよい。

【0166】

キー情報生成部23は、キー情報生成制御部23aを備える。キー情報生成制御部23aは、キー情報生成部23内部で生成された複数のキー情報を記憶する記憶部（図示せず）と、記憶部に記憶した複数のキー情報から1つのキー情報を選択する間隔の時間を計測するためのタイマを備える。

【0167】

キー情報生成制御部23aは、キー情報生成部23内部で生成された複数のキー情報を記憶部に記憶し、キー情報をコンテンツデータ受信装置30に送信する場合に、生成した複数のキー情報のそれぞれを暗号化し、暗号化した複数のキー情報を全て送信装置送受信部25に出力する。

【0168】

キー情報生成部23におけるキー情報の暗号化は、予め定められた方法により行われる。後述するコンテンツデータ受信装置30のキー情報抽出部33は、キー情報生成部23により行われたキー情報の暗号化を解除する復号処理機能を備え、キー情報生成部23が暗号化したキー情報は、後述するキー情報抽出部33により復号が可能である。本実施例では、キー情報生成部23がキー情報を暗号化してコンテンツデータ受信装置30に送信するが、暗号化せずにキー情報をコンテンツデータ受信装置30に送信するようにしてもよい。

【0169】

キー情報生成制御部23aは、記憶部に記憶した複数のキー情報のうち、コンテンツデータの暗号化に用いる1つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部

22に出力すると共に、選択したキー情報に関する選択情報を送信装置送受信部25に出力する。選択情報は、複数のキー情報のうちのどのキー情報であるかを示す情報であり、例えば、1、2の番号などである。キー情報生成制御部23aにおけるキー情報の選択方法は、特に限定されず、複数のキー情報を1番目から順番に選択してもよく、また、ランダムに選択してもよい。

【0170】

キー情報生成制御部23aは、コンテンツ再生部21においてコンテンツデータの再生が開始した時、記憶部に記憶した複数のキー情報のうちから1つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部22に出力すると共に、タイマにより時間の計測を開始する。キー情報を選択してから予め定めた時間の経過毎に、新たに、記憶部に記憶した他のキー情報のうちから1つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部22に出力する。コンテンツ暗号化部22は、キー情報生成部23から入力するあたらしいキー情報に基づいてコンテンツデータの暗号化を行う。また、キー情報生成部23は、キー情報を選択する毎に、選択したキー情報に関する選択情報を送信装置送受信部25に出力する。

【0171】

送信装置送受信部25は、前述した実施例のコンテンツデータ送信装置20の送信装置送受信部25の機能を備え、更に、キー情報送信データを送信する際に、キー情報生成部23から送られてきた複数のキー情報をキー情報送信データに格納してコンテンツデータ受信装置30に送信する。複数のキー情報をキー情報送信データに格納するとき、複数のキー情報を暗号化して格納してもよく、また、複数のキー情報のそれぞれを分割し、データの順番を入れ替えて複数のデータ列にそれぞれ格納してもよく、また、暗号化せずに格納してもよい。

【0172】

また、送信装置送受信部25は、コンテンツ暗号化部22から送られてきた暗号化コンテンツデータをコンテンツ送信データに格納して送信する際に、キー情報生成部23から入力する選択情報もコンテンツ送信データに格納し、コンテンツデータ受信装置30に送信する。選択情報は、コンテンツ送信データの第1データ列の第1送信データ情報領域～第6データ列の第6送信データ情報領域の全てに格納してもよく、また、いずれかに格納してもよい。

【0173】

このように本実施例のコンテンツデータ送信装置20は、キー情報生成部23において複数のキー情報を生成し、キー情報をコンテンツデータ受信装置30に送信する際に、キー情報送信データに複数のキー情報の全てを格納し、コンテンツデータ受信装置30に送信する。また、キー情報生成部23では、予め定めた時間毎に複数のキー情報の中から1つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部22に出力すると共に、選択したキー情報に関する選択情報を送信装置送受信部25に出力する。

【0174】

コンテンツ暗号化部22は、キー情報生成部23から予め定めた時間間隔毎に送られてくるキー情報に基づいてコンテンツデータを暗号化し、送信装置送受信部25に出力する。送信装置送受信部25は、コンテンツ暗号化部22から送られてくる暗号化コンテンツデータと、キー情報生成部23から送られてくるキー情報に関する選択情報とを、コンテンツ送信データに格納し、コンテンツデータ受信装置30に送信する。

【0175】

すなわち、コンテンツデータ送信装置20は、コンテンツデータを予め定めた時間毎に異なるキー情報で暗号化し、その暗号化コンテンツデータと暗号化に用いたキー情報に関する選択情報とをコンテンツデータ受信装置30に送信する。

【0176】

コンテンツデータ受信装置30は、受信装置送受信部31、受信装置ID認証部32、キー情報抽出部33、コンテンツ復号化部34、出力部35、受信装置制御部36を備え

る。このうち、受信装置 ID 認証部 32、コンテンツ復号化部 34、出力部 35、受信装置制御部 36 は、前述した実施例のコンテンツデータ受信装置 30 の受信装置 ID 認証部 32、コンテンツ復号化部 34、出力部 35 及び受信装置制御部 36 と同様であるため、説明を省略する。

【0177】

受信装置送受信部 31 は、前述した実施例の受信装置送受信部 31 の機能を備え、更に、コンテンツ送信データを受信した場合にコンテンツ送信データに含まれる選択情報をキー情報抽出部 33 に出力する処理を行う。

【0178】

キー情報抽出部 33 は、受信装置送受信部 31 が受信したキー情報送信データに格納されている複数のキー情報を抽出し、キー情報を取得する。キー情報抽出部 33 は、キー情報記憶部 33a を備え、取得したキー情報をキー情報記憶部 33a に格納する。

【0179】

キー情報抽出部 33 は、コンテンツデータ送信装置 20 からコンテンツ送信データが送られてきた際に、コンテンツ送信データに含まれる選択情報に基づいて、キー情報記憶部 33a に記憶している複数のキー情報から 1 つのキー情報を選択し、選択したキー情報をコンテンツ復号化部 34 に出力する。

【0180】

このようにコンテンツデータ受信装置 30 は、コンテンツデータ送信装置 20 から送られてきた複数のキー情報をキー情報記憶部 33a に記憶し、その後、暗号化コンテンツデータと共に送られてくる選択情報に基づいて、複数のキー情報の中から 1 つのキー情報を選択し、そのキー情報を用いて暗号化コンテンツデータを復号する。

【0181】

次に、本発明の他の本実施例のコンテンツデータ送受信システムにおけるデータの送受信の流れについて説明する。

図 6 において、コンテンツデータ送信装置 20 は、コンテンツデータ送信装置 20 とコンテンツデータ受信装置 30 とが信号線により接続されているか否かを確認するため、図 2 (a) に示す接続確認データを、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0182】

コンテンツデータ受信装置 30 は、受信装置送受信部 31 がコンテンツデータ送信装置 20 から送信された接続確認データを受信すると、図 2 (b) に示す接続確認応答データを受信装置送受信部 31 から応答線を介してコンテンツデータ送信装置 20 に送信する。

【0183】

コンテンツデータ送信装置 20 は、送信装置送受信部 25 がコンテンツデータ受信装置 30 から送信された接続確認応答データを受信すると、送信装置 ID 認証部 24 の送信 ID 記憶部 24a に記憶しているコンテンツデータ受信装置毎に固有に割り当てられている複数の受信装置 ID 情報から 1 つの受信装置 ID 情報を抽出し、抽出した受信装置 ID 情報を暗号化し、暗号化した受信装置 ID 情報を分割して図 3 (a) に示す機器認証データに格納し、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0184】

コンテンツデータ受信装置 30 は、受信装置送受信部 31 がコンテンツデータ送信装置 20 から送信された機器認証データを受信すると、機器認証データの中から ID 情報領域に格納されている受信装置 ID 情報を抽出し、抽出した受信装置 ID 情報を復号し、復号した受信装置 ID 情報と受信装置 ID 認証部 32 の受信 ID 記憶部 32a に記憶されている受信装置 ID 情報とを照合する。

【0185】

機器認証データから抽出した受信装置 ID 情報と受信 ID 記憶部 32a に記憶している受信装置 ID 情報とが一致した場合、コンテンツデータ受信装置 30 は、当該受信装置 ID

D情報を暗号化し、暗号化したデータを分割し、図3（b）に示す機器認証応答データに格納し、受信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0186】

機器認証データから抽出した受信装置ID情報と受信ID記憶部32aに記憶している受信装置ID情報とが一致しない場合、コンテンツデータ受信装置30は、受信ID情報が一致しない旨の情報（例えば、全て「0」のデータ）を暗号化し、暗号化したデータを分割して図3（b）に示す機器認証応答データに格納し、受信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0187】

コンテンツデータ送信装置20は、送信装置送受信部25がコンテンツデータ受信装置30から送信された機器認証応答データを受信すると、機器認証応答データに格納されているデータを抽出し、そのデータからコンテンツデータ受信装置30において受信情報ID情報が一致したか否か確認する。

【0188】

機器認証データから得たデータがコンテンツデータ受信装置30において受信装置ID情報が一致した旨の情報の場合、コンテンツデータ送信装置20は、キー情報生成部23において複数のキー情報を生成し、生成した複数のキー情報を暗号化し、暗号化したデータを分割して図4（a）に示すキー情報送信データに格納し、送信装置送受信部25から第1データ線～第6データ線を介してコンテンツデータ受信装置30に送信する。

【0189】

機器認証データから得たデータがコンテンツデータ受信装置30において受信装置ID情報が一致しない旨の情報の場合、コンテンツデータ送信装置20は、送信装置ID認証部24の送信ID記憶部24aに記憶している複数の受信装置ID情報の中から、既にコンテンツデータ受信装置30に送信した受信装置ID情報を除く受信装置ID情報の中から1つの受信装置ID情報を抽出し、その受信装置ID情報を暗号化し、暗号化したデータを分割して図3（a）に示す機器認証データに格納し、再度、送信装置送受信部25から第1データ線～第6データ線を介してコンテンツデータ受信装置30に送信する。コンテンツデータ送信装置20は、コンテンツデータ受信装置30に割り当てられた受信装置ID情報と一致するまでこの処理を繰り返し行う。

【0190】

コンテンツデータ受信装置30は、受信装置送受信部31がコンテンツデータ送信装置20から送信されたキー情報送信データを受信すると、キー情報送信データの中からキー情報領域に格納されているデータを抽出し、抽出したデータを復号化し、複数のキー情報を取得する。このキー情報を、キー情報記憶部32aに記憶する。

【0191】

キー情報送信データからキー情報を取得することができた場合、コンテンツデータ受信装置30は、キー情報を取得した旨の情報（例えば、全て「1」のデータ）を暗号化し、暗号化したデータを分割して図4（b）に示すキー情報受信データに格納し、受信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0192】

キー情報送信データからキー情報を取得できなかった場合、コンテンツデータ受信装置30は、キー情報を取得できなかった旨の情報（例えば、全て「0」のデータ）を暗号化し、暗号化したデータを分割して図4（b）に示すキー情報受信データに格納し、受信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0193】

コンテンツデータ送信装置20は、送信装置送受信部25がコンテンツデータ受信装置30から送信されたキー情報受信データを受信すると、キー情報受信データの受信データ領域に格納されているデータを抽出し、コンテンツデータ受信装置30がキー情報を取得したか否かを確認する。

【0194】

コンテンツデータ受信装置30においてキー情報を取得できなかった場合、コンテンツデータ送信装置20は、再度、キー情報送信データを送信装置送受信部25から第1データ線～第6データ線を介してコンテンツデータ受信装置30に送信する。

【0195】

コンテンツデータ受信装置30においてキー情報を取得できた場合、コンテンツデータ送信装置20は、コンテンツ再生部21においてコンテンツデータの再生を開始すると共に、キー情報生成部23においてコンテンツデータ暗号化に用いるキー情報の選択を行う。そして、コンテンツ暗号化部22において選択されたキー情報を用いてコンテンツデータを暗号化する処理を開始する。

【0196】

コンテンツデータ送信装置20は、コンテンツ暗号化部22により暗号化した暗号化コンテンツデータを分割し、分割したデータを図5(a)に示すコンテンツ送信データに格納し、また、キー情報生成部23から得られる選択情報をコンテンツ送信データに格納し、送信装置送受信部25から第1データ線～第6データ線を介してコンテンツデータ受信装置30に送信する。

【0197】

コンテンツデータ受信装置30は、コンテンツデータ送信装置20が送信したコンテンツ送信データを取得できなかった場合、コンテンツデータを取得できなかった旨の情報(例えば、全て「0」のデータ)を暗号化し、暗号化したデータを分割して図5(b)に示すコンテンツ受信データに格納し、受信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0198】

コンテンツデータ受信装置30は、受信装置送受信部31がコンテンツデータ送信装置20から送信されたコンテンツ送信データを受信すると、コンテンツ送信データに格納されている選択情報を抽出してキー情報抽出部33に出力すると共に暗号化コンテンツデータをコンテンツ復号化部34に出力する。キー情報抽出部33は、選択情報に基づいてキー情報記憶部33aに記憶されている複数のキー情報から1つのキー情報を選択する。そして、コンテンツ復号化部34は、キー情報抽出部33が選択したキー情報を用いて暗号化コンテンツデータを復号化し、出力部35に出力する。

【0199】

出力部35は、コンテンツ復号化部34から出力されたコンテンツデータに対して、デジタルアナログ変換や増幅等を行い出力する。

【0200】

コンテンツデータ受信装置30は、コンテンツデータ送信装置20が送信したコンテンツ送信データを受信し暗号化コンテンツデータを復号すると、暗号コンテンツデータを取得した旨の情報を暗号化し、暗号化したデータを分割して図5(b)に示すコンテンツ受信データに格納し、送信装置送受信部31から応答線を介してコンテンツデータ送信装置20に送信する。

【0201】

コンテンツデータ送信装置20は、コンテンツデータ受信装置30から送信されたコンテンツ受信データを受信すると、コンテンツ受信データに格納されているコンテンツデータを取得した旨の情報からコンテンツデータ受信装置30がコンテンツデータを取得できたか否かを確認する。

【0202】

コンテンツデータ送信装置20は、コンテンツデータ受信装置30がコンテンツデータを取得できた場合、次の暗号化コンテンツデータを図5(a)に示すコンテンツ送信データに格納し、コンテンツ送信データを送信装置送受信部25から第1データ線～第6データ線を介してコンテンツデータ受信装置30に送信する。

【0203】

コンテンツデータ送信装置 20 は、コンテンツデータ受信装置 30 がコンテンツデータを取得できなかった場合、送信したコンテンツ送信データを、再度、送信装置送受信部 25 から第 1 データ線～第 6 データ線を介してコンテンツデータ受信装置 30 に送信する。

【0204】

コンテンツデータ送信装置 20 は、キー情報生成部 23 のキー情報生成制御部 23a において新たにキー情報が選択された場合、コンテンツ暗号化部 22 において新たに選択されたキー情報に基づいてコンテンツデータの暗号化を行い、その暗号化コンテンツデータを送信する際にコンテンツ送信データに新たに選択したキー情報に関する選択情報を格納し、コンテンツデータ受信装置 30 に送信する。

【0205】

コンテンツデータ受信装置 30 は、キー情報抽出部 33 においてコンテンツ送信データに格納されている新たな選択情報に基づいてキー情報記憶部 33a に記憶している複数のキー情報の中から前記選択情報に基づいて 1 つのキー情報を選択し、コンテンツ復号化部 34 においてキー情報抽出部 33 から得た新たなキー情報を用いて暗号化コンテンツデータを復号化する。

【0206】

このようにして、コンテンツデータ送信装置 20 からコンテンツデータ受信装置 30 にコンテンツデータを送信する。

【0207】

他の実施例のコンテンツデータ送受信システムにおいては、コンテンツデータの暗号化に用いるキー情報を複数生成し、複数のキー情報の中から選択した 1 つのキー情報を用いてコンテンツデータを暗号化してコンテンツデータ受信装置に送信することができるため、不正にキー情報、暗号化コンテンツデータを取得することが困難になり、暗号化コンテンツデータをキー情報を用いて復号してコンテンツデータの違法複製することを防止することができる。

【0208】

以上のように、本発明のコンテンツデータ送受信システムでは、コンテンツデータ送信装置とコンテンツデータ受信装置との間で、機器認証を行うための受信装置 ID 情報、暗号化コンテンツデータを復号するためのキー情報、暗号化したコンテンツデータを、複数のデータ列からなるそれぞれのデータに格納し、そのデータを複数の信号線を用いてコンテンツデータ受信装置に送信する。このため、コンテンツデータ送信装置が出力する受信装置 ID 情報、キー情報、暗号化コンテンツデータを単一の信号線から取得することができないため、不正に受信装置 ID 情報、キー情報、暗号化コンテンツデータを得て、暗号化コンテンツデータをキー情報を用いて復号してコンテンツデータの違法複製を防止することができる。

【0209】

上述した実施例においては、コンテンツデータ送信装置からコンテンツデータ受信装置にデータを送信する信号線を 6 本の信号線（第 1 データ線～第 6 データ線）として説明したが、2 本以上の多数の信号線であればいずれの本数でもよい。

【0210】

コンテンツデータ送信装置からコンテンツデータ受信装置にデータを送信する信号線の本数を多いことにより、受信装置 ID 情報及びキー情報を分割する数が増えるため、信号線から受信装置 ID 情報及びキー情報を不正に取得しにくくすることができる。また、暗号化コンテンツデータも同様に取得しにくくできると共に、より多くのチャンネル数のオーディオデータを送信することも可能になる。

【0211】

また、上述した実施例では、コンテンツデータ送信装置からコンテンツデータ受信装置に接続確認データ、機器認証データ、キー送信データ、コンテンツ送信データを送信する際に、コンテンツデータ送信装置は、複数のデータ列を同時に送信しているが、複数のデータ列を時間差を設けて送信してもよい。すなわち、第 1 データ列を送信した後、予め定

めた時間経過後に第2データ列を送信し、同様に、第3データ列～第6データ列を時間差を設けて送信するようにしてもよい。

【0212】

このことにより、コンテンツデータ送信装置が送信したデータを同時刻に受信し、同時刻に受信したデータに格納されている情報の組み替えを行っただけでは、当該データに格納されている情報から正しい情報（例えば、受信装置ID情報、キー情報など）を取得することが困難になる。したがって、コンテンツデータ送信装置が出力する受信装置ID情報、キー情報、暗号化コンテンツデータを不正に取得し、そのデータを用いて暗号化コンテンツデータを復号してコンテンツデータを違法に複製することを防止することができる。

【図面の簡単な説明】

【0213】

【図1】本発明のコンテンツデータ送受信システムの一実施例を示す概略構成図。

【図2】本実施例のコンテンツデータ送受信システムにおける接続確認データ及び接続確認応答データのフォーマットを示す図。

【図3】本実施例のコンテンツデータ送受信システムにおける機器認証データ及び機器認証応答データのフォーマットを示す図。

【図4】本実施例のコンテンツデータ送受信システムにおけるキー情報送信データ及びキー情報受信データのフォーマットを示す図。

【図5】本実施例のコンテンツデータ送受信システムにおけるコンテンツ送信データ及びコンテンツ受信データのフォーマットを示す図。

【図6】本発明のコンテンツデータ送受信方法の一実施例を説明するための図。

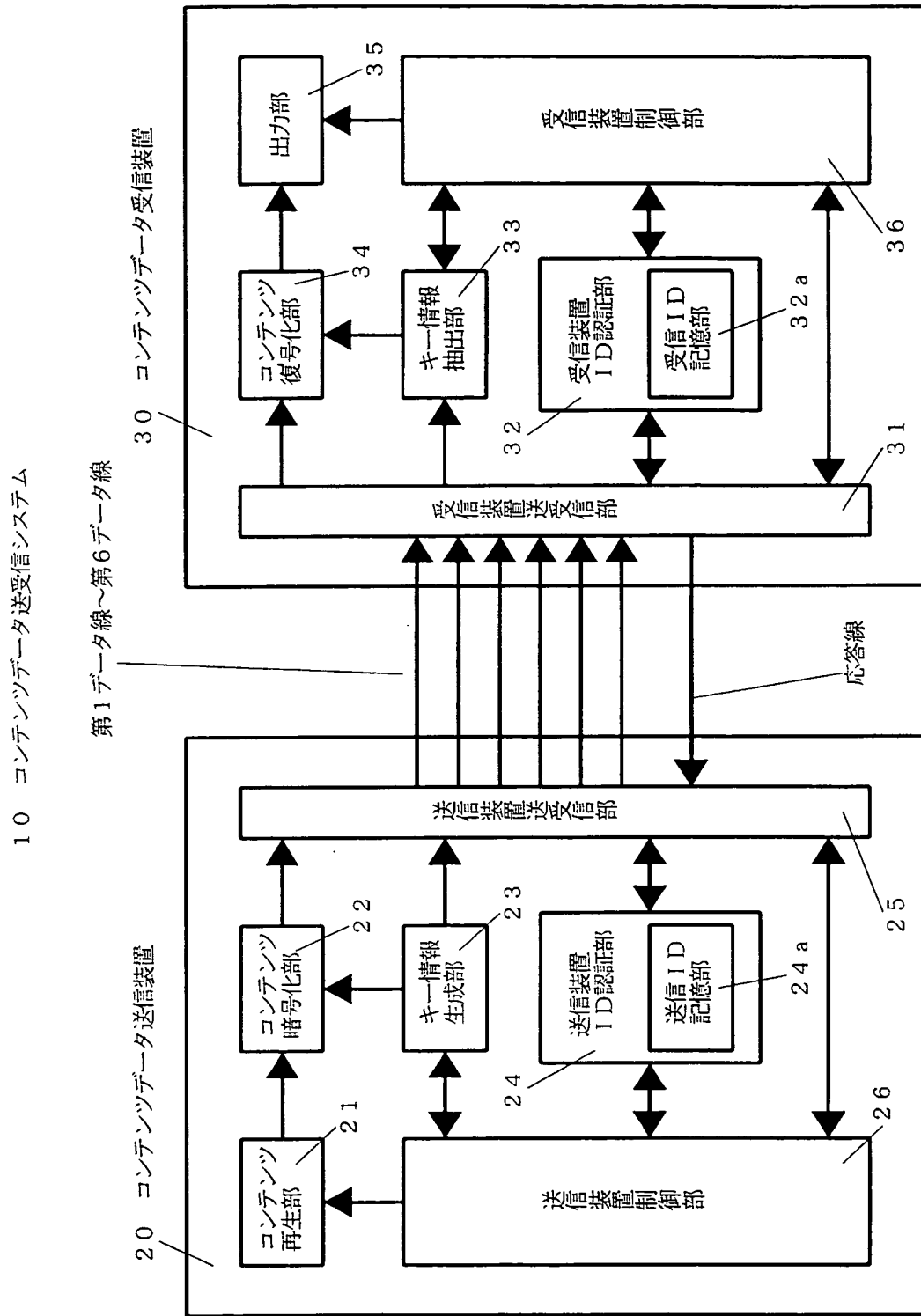
【図7】本発明のコンテンツデータ送受信システムの他の実施例を示す概略構成図。

【符号の説明】

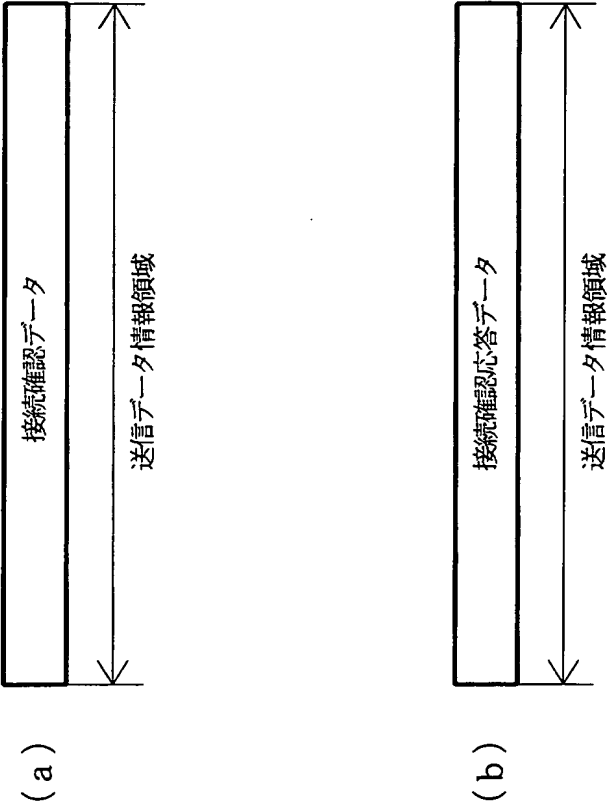
【0214】

10・・・コンテンツデータ送受信システム、20・・・コンテンツデータ送信装置、21・・・コンテンツ再生部、22・・・コンテンツ暗号化部、23・・・キー情報生成部、23a・・・キー情報生成制御部、24・・・送信装置ID認証部、24a・・・送信ID記憶部、25・・・送信装置送受信部、26・・・送信装置制御部、30・・・コンテンツデータ受信装置、31・・・受信装置送受信部、32・・・受信装置ID認証部、32a・・・受信ID記憶部、33・・・キー情報抽出部、33a・・・キー情報記憶部、34・・・コンテンツ復号化部、35・・・出力部、36・・・受信装置制御部。

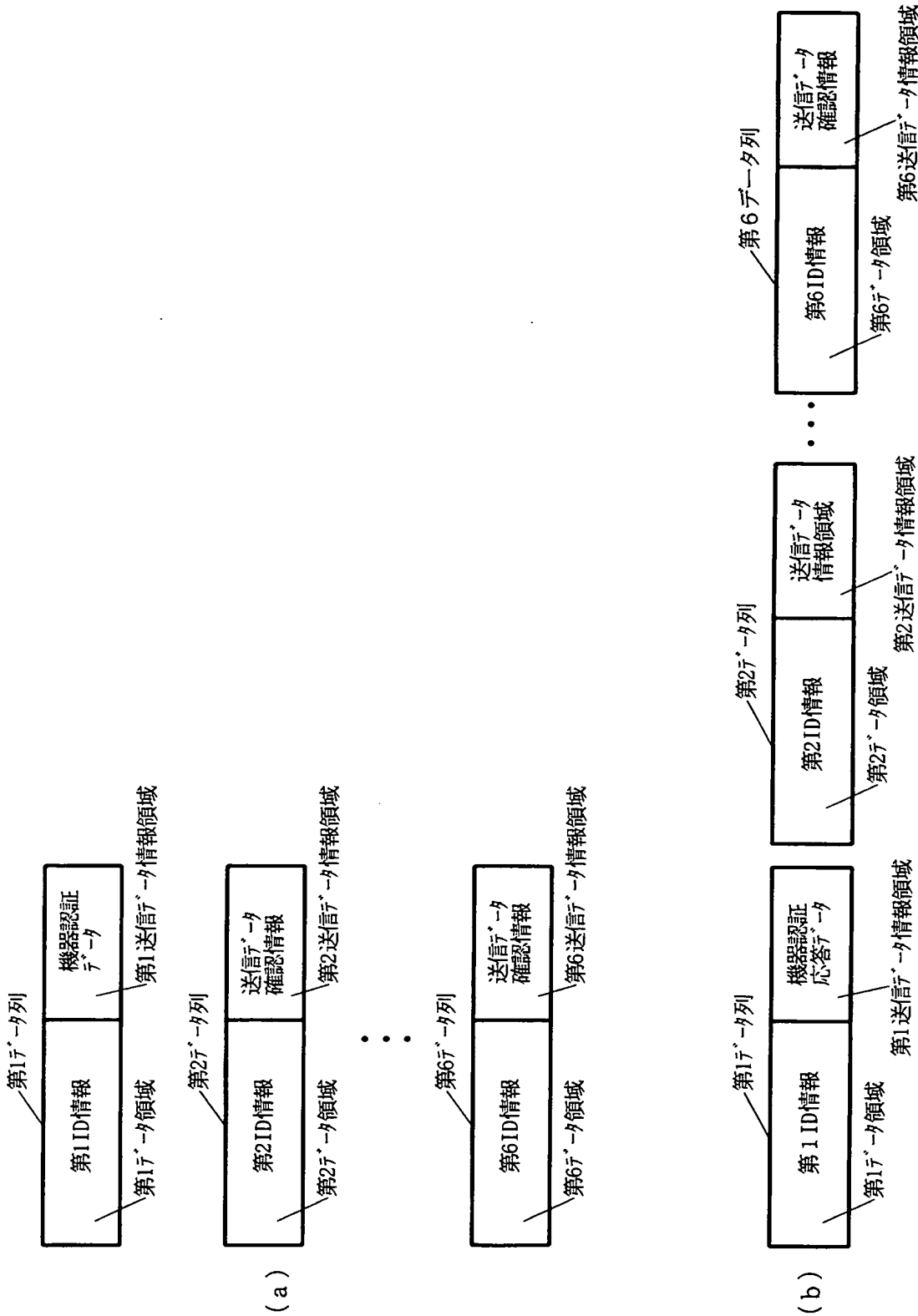
【書類名】 図面
【図 1】



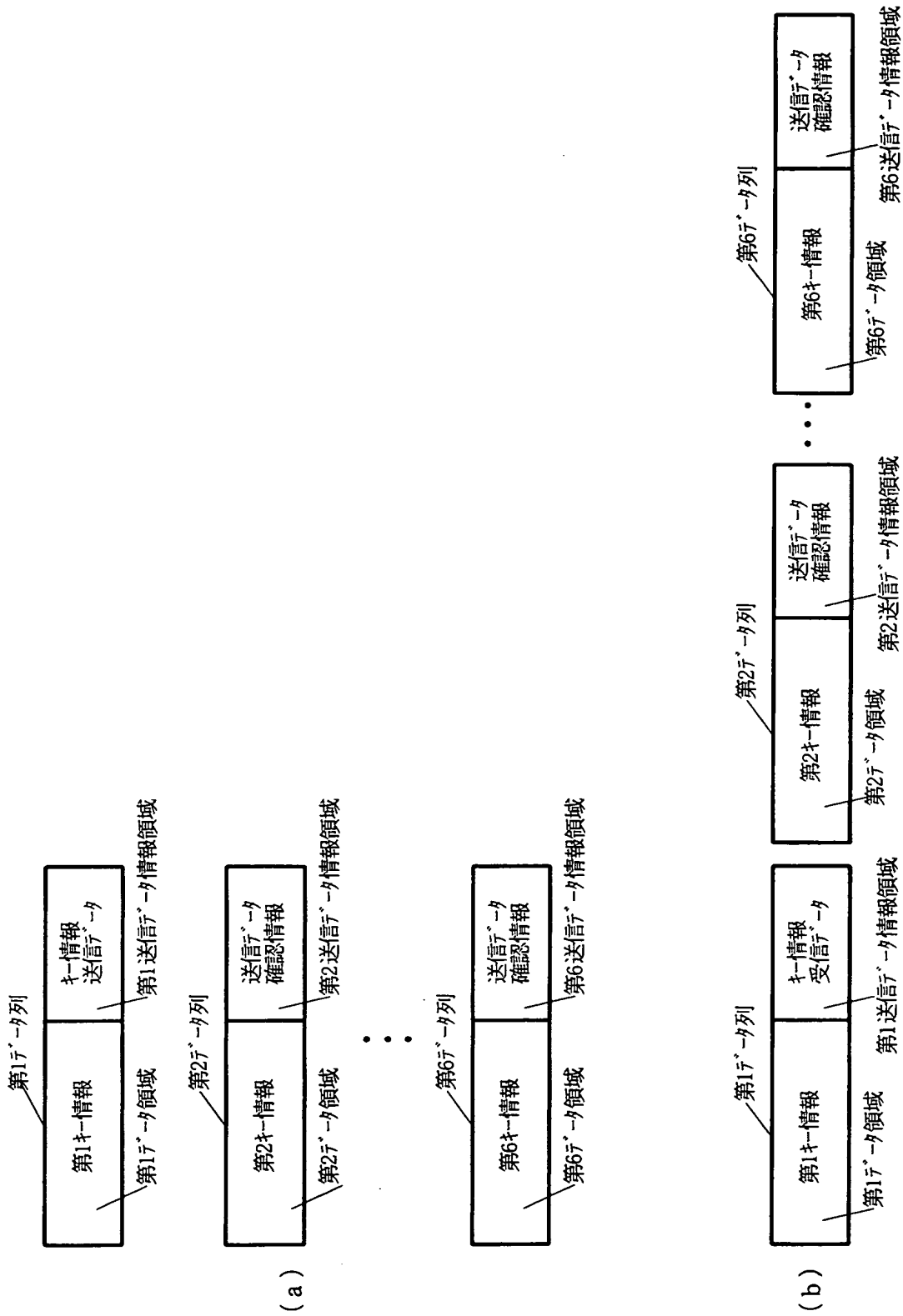
【図 2】



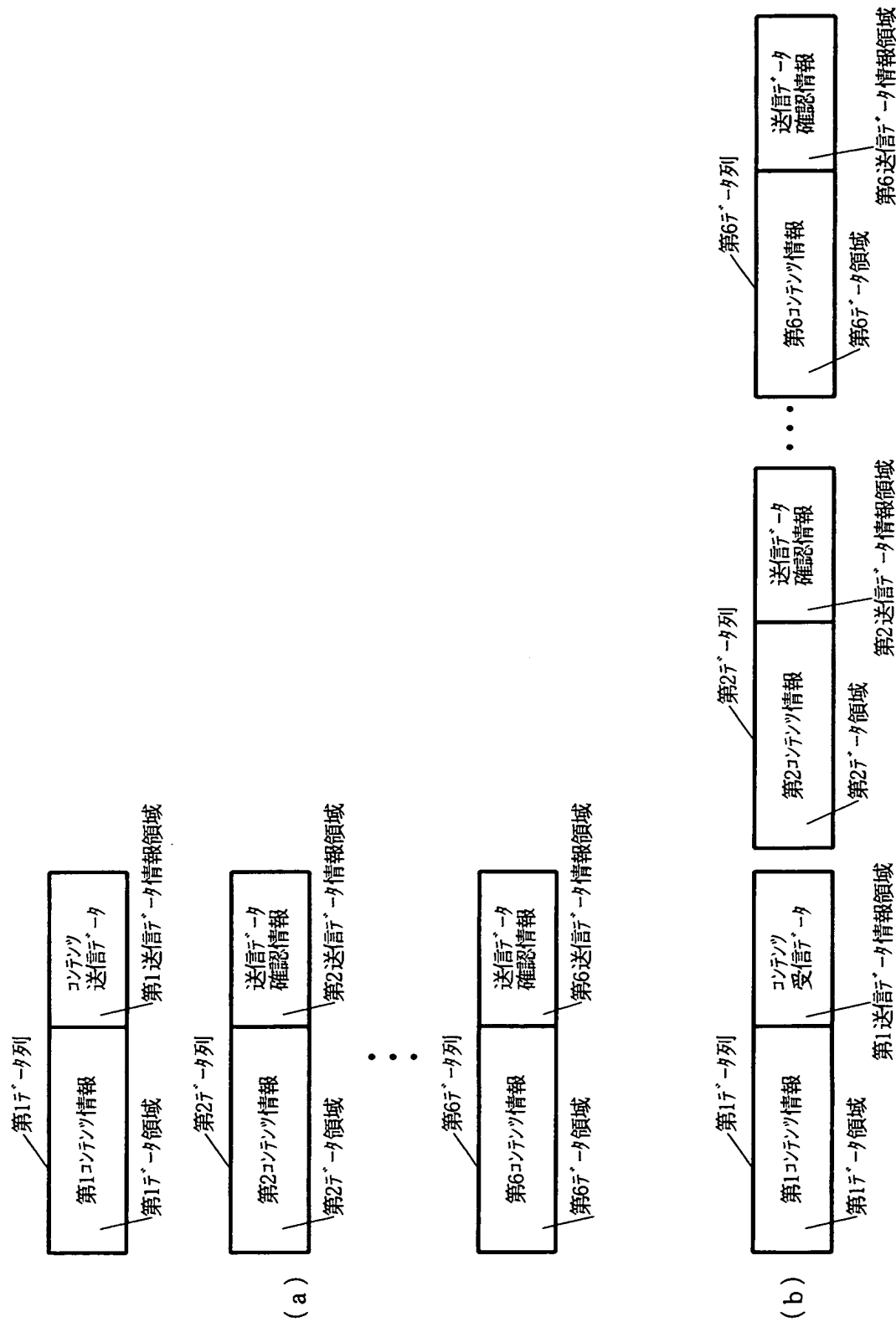
【図 3】



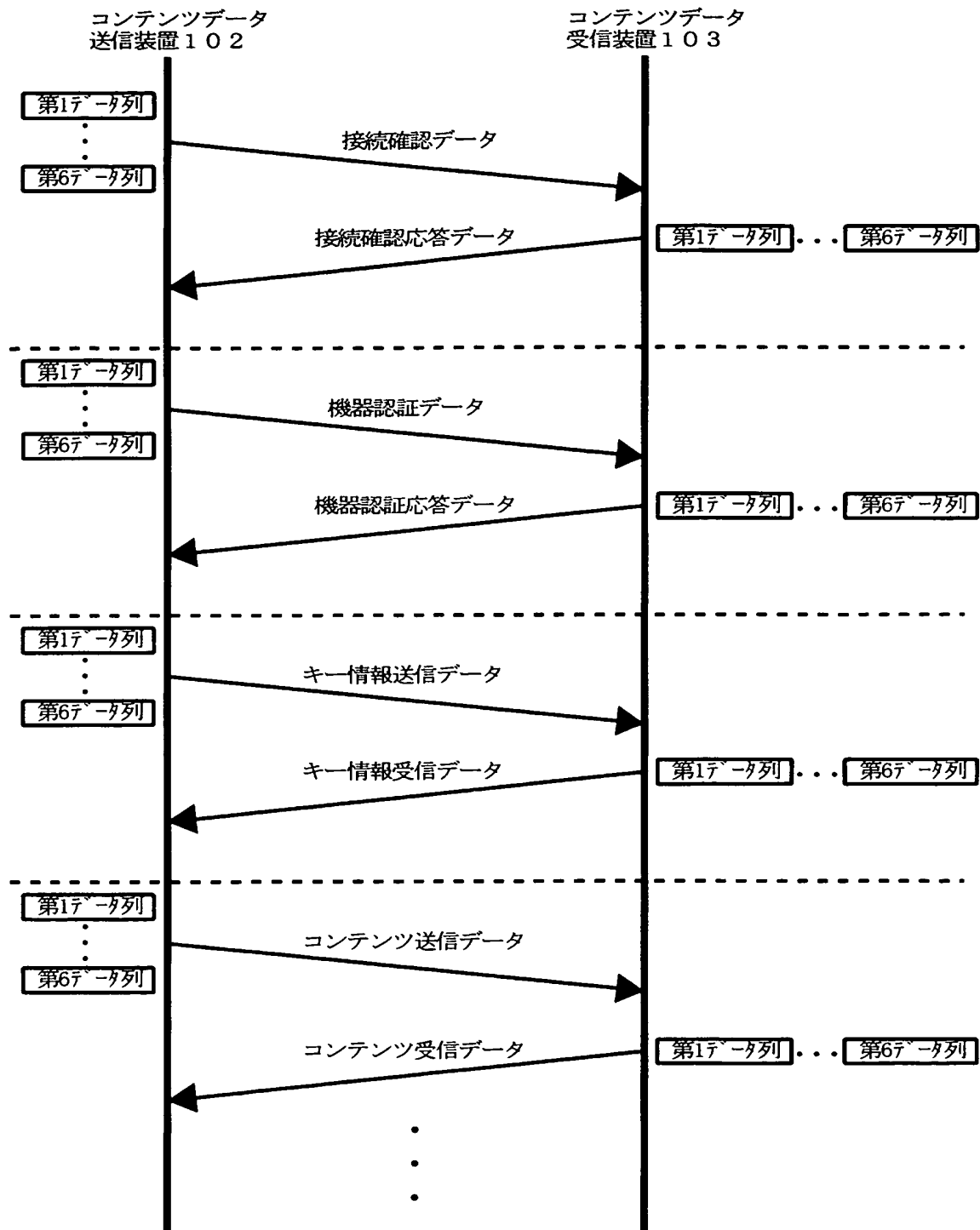
【図 4】



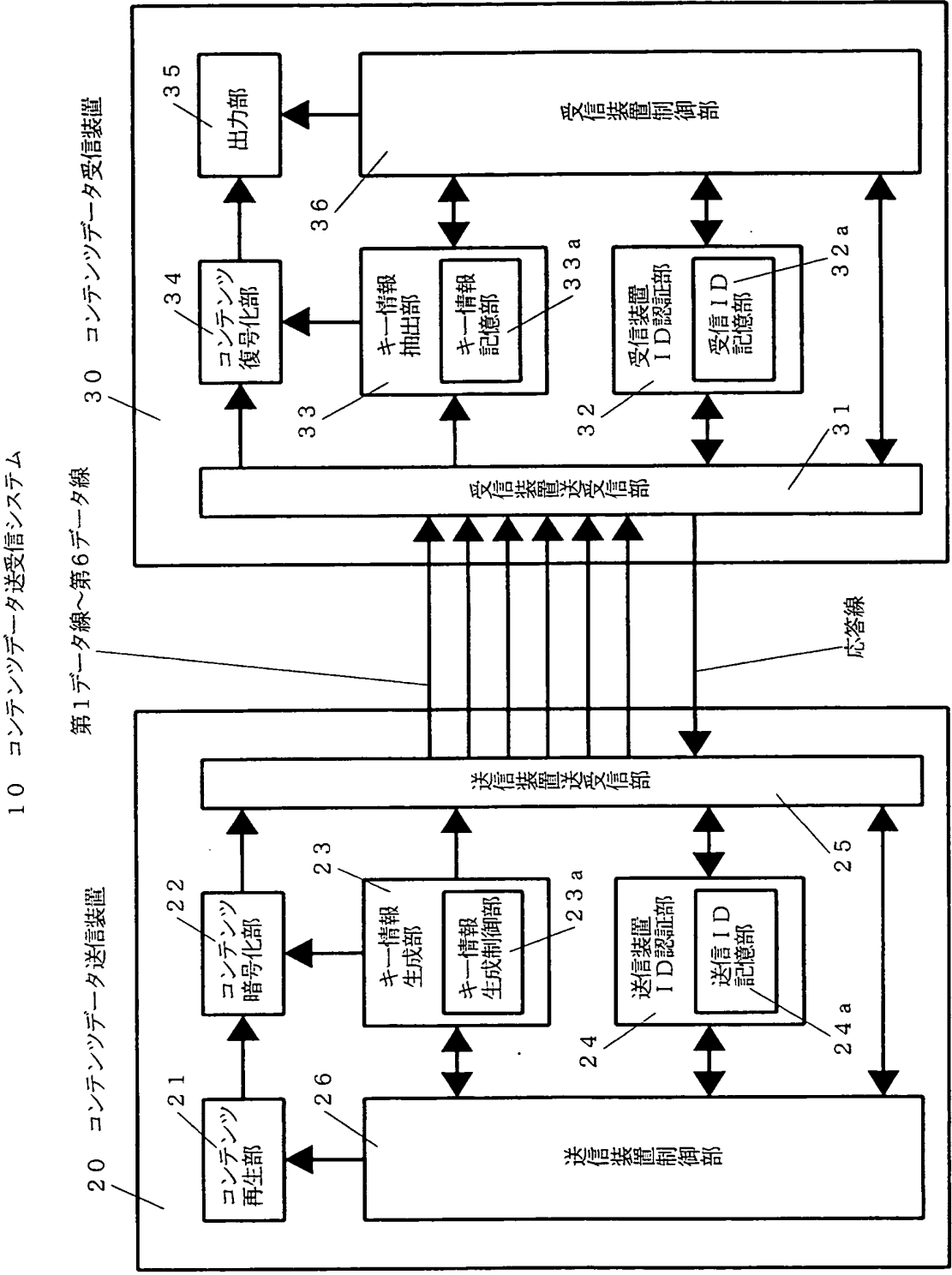
【図 5】



【図 6】



【図 7】



【書類名】 要約書**【要約】**

【課題】 コンテンツデータ送受信システムでは、2 台の装置を接続している単一の信号線を伝送しているデータから暗号解除情報を抽出し、暗号解除情報を用いて暗号化コンテンツデータを復号して元の高品質のコンテンツデータを得ることができるという問題がある。

【解決手段】 コンテンツデータ送受信システムにおいて、コンテンツデータ送信装置は、コンテンツデータをキー情報を用いて暗号化し、キー情報を信号路を介してコンテンツデータ受信装置に送信した後にそのキー情報によって暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する。コンテンツデータ受信装置は、コンテンツデータ送信装置から信号路を介して送信されたキー情報を取得し、コンテンツデータ送信装置から複数の信号路を介して送信された暗号化したコンテンツデータを受信し、キー情報を用いて前記暗号化したコンテンツデータを復号する。

【選択図】 図 1

特願 2 0 0 3 - 3 1 3 8 5 2

出 願 人 履 歴 情 報

識別番号

[3 0 1 0 6 6 0 0 6]

1. 変更年月日

2 0 0 1 年 1 0 月 9 日

[変更理由]

新規登録

住 所

東京都文京区湯島三丁目 1 6 番 1 1 号

氏 名

株式会社デノン